NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

LOCAL AREA NETWORK STANDARDS
AND GUIDELINES FOR
THE REPUBLIC OF CHINA NAVY (ROCN)

by

Wang-Nai

June 1988

Thesis Advisor: Judith H. Lind

Approved for public release; distribution is unlimited

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION
UNCLASSIFIED

1b. RESTRICTIVE MARKINGS

2a. SECURITY CLASSIFICATION AUTHORITY

2b. DECLASSIFICATION / DOWNGRADING SCHEDULE

3. DISTRIBUTION / AVAILABILITY OF REPORT
Approved for public release; distribution is unlimited

4. PERFORMING ORGANIZATION REPORT NUMBER(S)

5. MONITORING ORGANIZATION REPORT NUMBER(S)

6a. NAME OF PERFORMING ORGANIZATION
Naval Postgraduate School

6b. OFFICE SYMBOL *(If applicable)*
62

7a. NAME OF MONITORING ORGANIZATION
Naval Postgraduate School

6c. ADDRESS *(City, State, and ZIP Code)*
Monterey, California 93943-5000

7b. ADDRESS *(City, State, and ZIP Code)*
Monterey, California 93943-5000

8a. NAME OF FUNDING / SPONSORING ORGANIZATION

8b. OFFICE SYMBOL *(If applicable)*

9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER

8c. ADDRESS *(City, State, and ZIP Code)*

10. SOURCE OF FUNDING NUMBERS

PROGRAM ELEMENT NO	PROJECT NO	TASK NO	WORK UNIT ACCESSION NO

11. TITLE *(Include Security Classification)*
LOCAL AREA NETWORK STANDARDS AND GUIDELINES FOR THE REPUBLIC OF CHINA NAVY (ROCN)

12. PERSONAL AUTHOR(S)
WANG-Nai

13a. TYPE OF REPORT
Master's Thesis

13b. TIME COVERED
FROM ______ TO ______

14. DATE OF REPORT *(Year, Month, Day)*
1988 June

15. PAGE COUNT
68

16. SUPPLEMENTARY NOTATION The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

17. COSATI CODES

FIELD	GROUP	SUB-GROUP

18. SUBJECT TERMS *(Continue on reverse if necessary and identify by block number)*
data communication, protocols, switching technology media topologies, architecture and design of local area network (LAN), optimal LAN for ROCN

19. ABSTRACT *(Continue on reverse if necessary and identify by block number)*
This thesis provides a specific outline for Republic of China Navy (ROCN) Local Area Network (LAN) development. The current ROCN communication system and its problems are discussed, along with basic concepts of data communication, protocols, standards, and topologies. Token ring and Ethernet topologies are discussed in detail. Objectives and requirements for ROCN LAN systems are documented. These factors, plus security, budget, training and maintenance, reliability, efficiency, survivability, and performance are considered in proposing a methodology for ROCN LAN development.

20. DISTRIBUTION / AVAILABILITY OF ABSTRACT
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS

21. ABSTRACT SECURITY CLASSIFICATION
UNCLASSIFIED

22a. NAME OF RESPONSIBLE INDIVIDUAL
Judith H. Lind

22b. TELEPHONE *(Include Area Code)*
408-646-2594

22c. OFFICE SYMBOL
55Li

DD FORM 1473, 84 MAR

83 APR edition may be used until exhausted
All other editions are obsolete

☆ U.S. Government Printing Office: 1986—606-243

Approved for public release; distribution is unlimited.

Local Area Network
Standards and Guidelines for the Republic of China Navy

by

Wang-Nai
Lieutenant, Republic of China Navy
B.S., Republic of China Naval Academy, 1980

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN TELECOMMUNICATION SYSTEMS
MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
June 1988

Author: ______________________

Wang-Nai

Approved by: Judith H. Lind

Judith H. Lind, Thesis Advisor

Dan C Boger

Dan C. Boger, Second Reader

David R. Whipple, Chairman,
Department of Administrative Sciences

James M. Fremgen, Acting Dean of
Information and Policy Sciences

ABSTRACT

This thesis provides a specific outline for Republic of China Navy (ROCN) Local Area Network (LAN) development. The current ROCN communication system and its problems are discussed, along with basic concepts of data communication, protocols, standards, and topologies. Token ring and Ethernet topologies are discussed in detail. Objectives and requirements for ROCN LAN systems are documented. These factors, plus security, budget, training and maintenance, reliability, efficiency, survivability, and performance are considered in proposing a methodology for ROCN LAN development.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

I. INTRODUCTION

A. BACKGROUND: COMPUTER DEVELOPMENT

1. General

The modern world is experiencing many changes. This is notable especially in the increased use of electronics and computers. Although the computer industry is a young industry compared to other industries, it has seen great advances. The merging of computers and communication systems recently has had a great influence on the way computer systems are organized.

As the computer and communications industries evolve with the development of new technology, these technology areas are rapidly coverging. Techniques for collecting, transporting, storing, and processing data are also changing. As our capability to gather, process, and distribute information grows, the demand for even more sophisticated information processing grows faster.

2. History

The data processing industry began in the 1950s. Until terminals were first wired to telephone lines for purposes of sending data to a remotely located computer in the mid-1950s, the communications industry was oriented strictly toward voice communications. The development of the data processing industry opened the doors of the world of data communications. [Ref. 1: p. 176]

Further technological developments resulted in time-shared computer systems. Relatively large numbers of terminals then could be connected to a single computer, using the transmission facilities of the voice telephone network. [Ref. 1: p. 178]

The late 1960s also brought the development of common-plug peripheral devices. The manufacturers of plug-compatible equipment identified and exploited a market for peripherals, including multiplexers, concentrators, and terminals that could be connected with various computers and made available to users as alternatives to a single-vendor computer system arrangement. In the early 1970s, computer network complexity increased when coaxial cable and communication devices (multi-drop lines, multiplexors, concentrators, and intelligent terminal devices) were used to enchance and extend communications between users and the central processing unit (CPU). [Ref. 1: p. 178]

3. Trends for the Future

The use of small, dedicated minicomputers or microcomputers at remote locations, in place of mainframe computers, is perhaps the most significant computer development for this study. Although large mainframe computers are suitable for applications involving large data bases or requiring high-speed processing, many typical user functions do not need the speed and sophistication of such large computers. The result has been the increasing use of minicomputers at various user locations to replace a single large mainframe computer. In some applications microcomputers have been custom designed by the user to perform specialized functions in the most efficient manner at the remote location. [Ref. 2: p. 11]

A local area network (LAN) is a data communications system that allows communication between a number of independent devices (minicomputers and microcomputer). The network may support a wide variety of applications, such as file editing and transfer, electronic mail, and database mangement. [Ref. 3: p. 15]

Stand-alone small business computers and word processing systems also have evoved as important components in data processing networks, including LANs. Such systems may process text or data in a stand-alone mode, and then operate in a communications mode to transmit portions of the processed text or data to a remote computer for futher handling. Another mode of operation is for a given system to act in a distributed-intelligence mode: one computer transmits information to another system, which then performs additional processing. For example, programs or parameters supplied by the first computer may be used with data or text entered on the second computer at the remote location. [Ref. 2: p. 55]

B. THE REPUBLIC OF CHINA NAVY

1. Background

Since World War II China has been divided into two sections. One is free China, the Republic of China (ROC), Taiwan. The other is communist China, on the mainland of China. There is no formal relationship between the two countries (see Figure 1 on page 3).

The ROC on Taiwan has for more than 30 years been the Western Pacific center for resisting Communist China expansion. This country also provides positive contributions to the maintenance of peace for the Asian-Pacific region and the world. At the same time, the ROC is dedicated to the reconstruction of the nation of China under one free government.

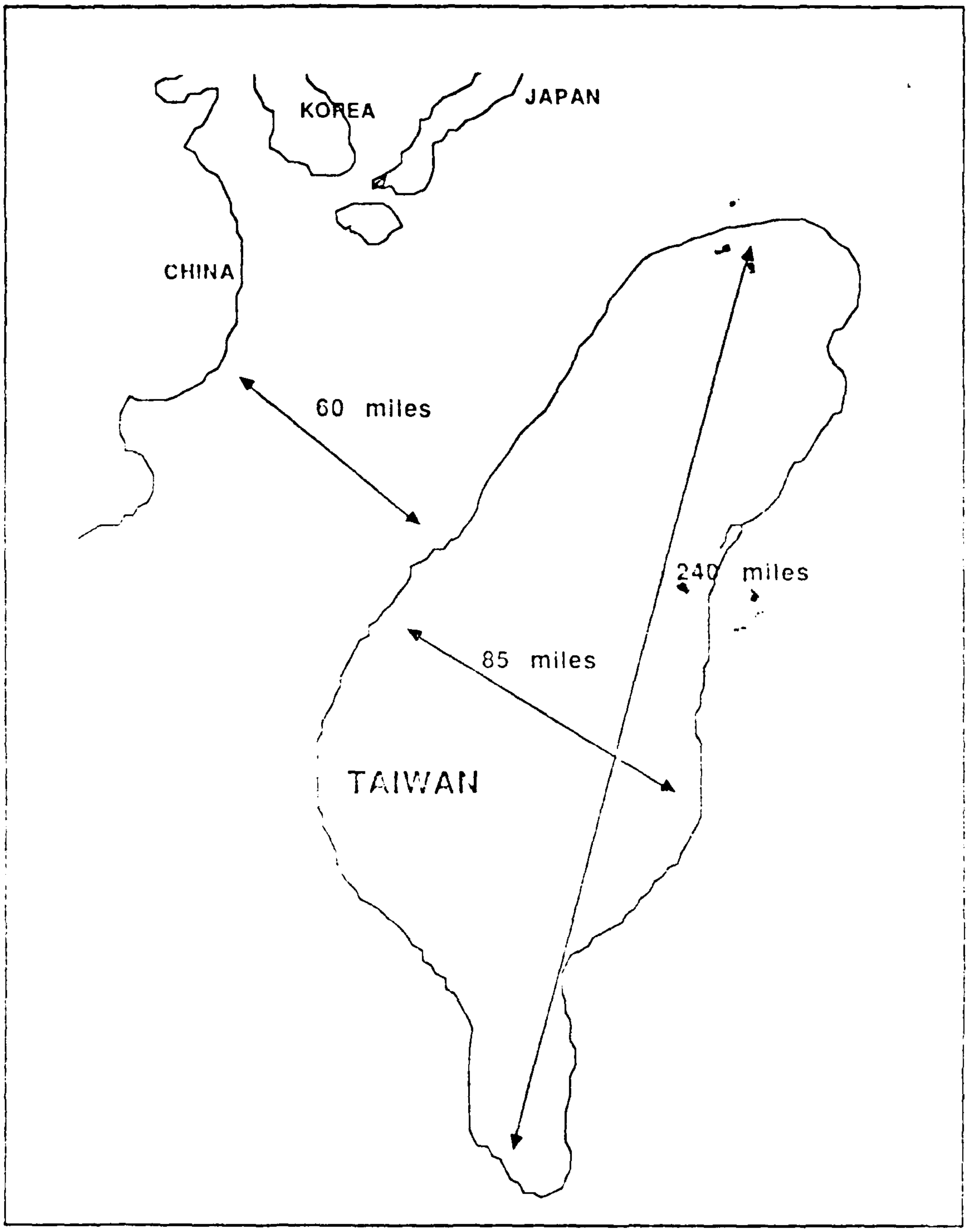


Figure 1. Taiwan and China

In addition to resisting communist China expansion, the government is involved in raising the living and cultural standard of its people. The country's strong Armed Forces--Army, Navy, and Air Force--are necessary to achieve both goals: defending against communist aggression and providing improved technology for everyday life (see Figure 2 on page 5).

2. Problem

The ROC Army, Navy, and Air Force each presently has its own communication system in Taiwan. Each system works independently. Development of an integrated communication system is important for the future of the country. The three communication systems all operate on the same basic concept. If one of the three services were to develop an integrated communication system, the others then could use that system or a similar one.

The ROC Navy (ROCN) is a medium sized organization, compared to the Army and Air Force. Normally communication is by telephone, radio, postal service, etc. Increasing the use of computers for communication, integrated, rapid data exchange, and accurate information processing are important goals for the modern Navy.

Many organizations within the ROCN are seeking ways to improve knowledge sharing and document management and delivery. ROCN divisions (fleet) presently do not use computers on a routine basis. Yet the need for data communication increases daily. Considering the demanding requirements of a heterogenous ROCN user population, the improving cost-effectiveness of smaller, dedicated processors for specialized tasks, and the increasing availability of computer networking facilities, the development of LANs for ROCN divisions should be seriously considered.

As increased successes on the part of the computer combine with the growing needs of user communities, the importance of data communications will continue to increase. In particular, the development of LANs will be an important trend in future computer development. Serious consideration should be given to implementing LANs for each ROCN division.

C. GOALS AND OBJECTIVES

1. Goals

This study will provide a specific outline for ROCN LAN development. Anticipated division acceptance of LAN systems will be discussed, along with LAN impact on future shipboard communication. The goals of this study are :

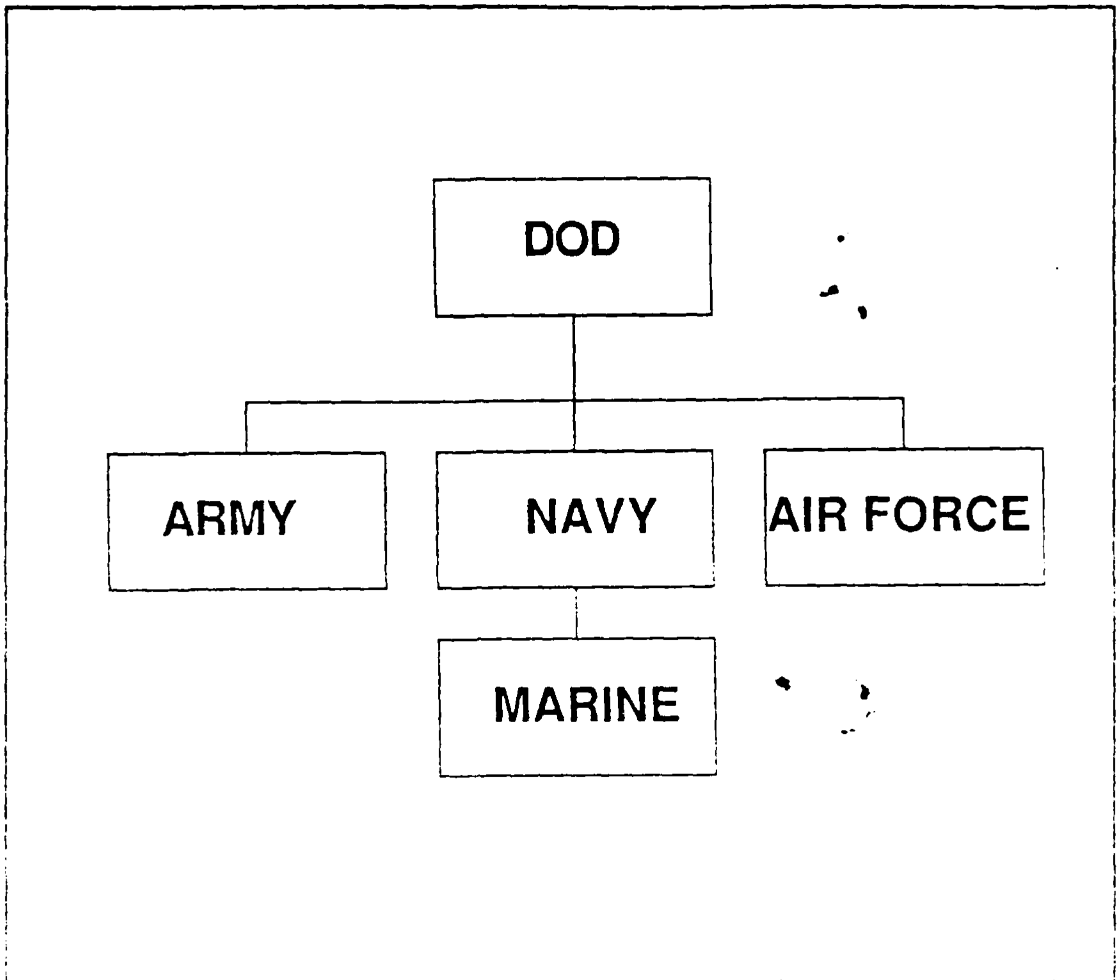


Figure 2. **The ROC Department of Defense Structure**

- Determine the impact of LAN systems on future shipboard communication, on work efficiency, and on warfighting capability.
- Describe possible effects and advantages of LANs for both civilians and the military in Taiwan.
- Propose future plans for connecting Navy local and long distance networks for defense network applications.

2. Study Objectives

In order to achieve these goals, the following objectives must be met.

- Describe the current communication system of the ROCN, focused on the division level.
- Define the requirements for an effective LAN for the ROCN.

- Discuss how LANs can support the communication needs of ROCN divisions.
- Propose a model that could be used for ROCN LANs based on United States systems.

D. THESIS OUTLINE

The basic concept of data communication is discussed in Chapter II. This includes such things as communications media, topologies, etc. Chapter III covers current existing LAN protocols, standards, approaches, interconnection issues, etc. Two popular model LAN designs also are provided there. ROCN LAN objectives and ROCN LAN goals are covered in Chapter IV, along with information and networking requirements that may be used to determine whether the LAN is the appropriate technology for the ROCN division. Chapter V provides conclusions based on this study.

II. DATA COMMUNICATION

A. DEFINITION OF A LAN

Local area networks, normally referred to simply as LANs, are interconnected distributed communities of computer-based data terminal equipment. This equipment normally is confined to a single building or localized group of buildings. For example, a LAN may be used to interconnect a community of computer-based workstations distributed around a block of offices within a building. Alternatively, it may be used to interconnect various computer-based items of equipment located within a single organization. [Ref. 4: p. 202]

LANs are normally installed and maintained by one organization; hence they are also referred to as private data networks [Ref. 4: p. 202]. Networks accessed by numerous organizations are called public data networks. There is a major difference between a commmunications path established using a LAN and a connection made through a public data network. With a LAN, because of the relatively short distance between the various items of interconnected equipment, much higher data transmission rates are normally possible. [Ref. 4: p. 203]

In summary, LANs have three identifying characteristics:

1. Networks range from a few hundred yards to about 30 miles, connecting computer-based data terminals.
2. Communications occur at a high data rate, up to 10 million bits per second.
3. LANs are owned and operated by a single organization.

B. OPEN SYSTEMS INTERCONNECTION MODEL

Many different communications systems and kinds of equipment are used throughout the world. This has created the need for standards and protocols that allow different brands of computers to communicate and to transfer data between various nodes. The International Standards Organization (ISO) has responded to this need by standardizing a multilayered computer architecture that permits interoperability between computer systems. The ISO standard uses what is called the Open Systems Interconnection (OSI) model. This model divides computer architecture into seven layers and prescribes protocols for each layer (see Figure 3 on page 8). [Ref. 4: p. 203]

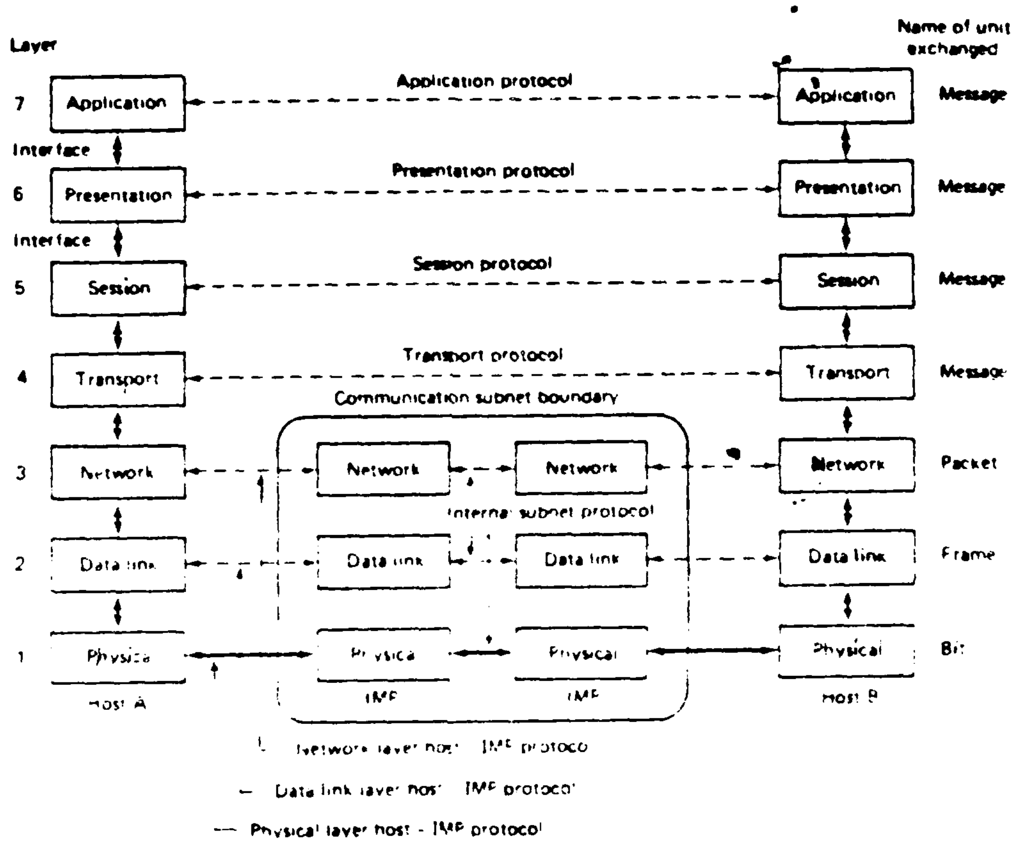


Figure 3. The Open Systems Interconnection Model for Standard Communication Protocols

Only the lowest layer provides for actual physical connections. That is, only this layer is concerned with an actual exchange of raw bits over a communication channel. In all the others only logical connections are created, with data sent from layer to layer in order to get it across to another system. The seven layers are described below.

1. Layer 1: Physical Layer

This layer defines the physical interface between devices and the rules by which bits are passed from one to another. It is used in prescribing the interface between data terminal equipment and data circuit terminating equipment. In addition, the number of signal lines and the shape and the size of connectors are specified by the physical layer standards.

2. Layer 2: Data Link Layer

The task of the data link layer is to take raw data transmissions and transform them so they are free of transmission errors and can be used by the network layer (layer 3). This is accomplished by breaking the input data into data frames, transmitting the frames sequentially, and processing acknowledgement frames sent back by the receiver.

3. Layer 3: Network Layer

This layer basically divides data streams into packets for transfer between a host and a network and between network components. Using these protocols, messages are accepted from a source host and coverted to packets. Packets then are directed toward their destinations.

4. Layer 4: Transport Layer

The basic function of the transport layer (also known as the host-to-host layer) is to accept data from the session layer (layer 5), split it up into smaller units if necessary, pass these to the network layer (layer 4), and ensure that the pieces all arrive correctly at the other end.

5. Layer 5: Session Layer

This layer provides an end-to-end procedure that establishes, maintains, and terminates logical relationships between processes in the higher layers. It is the user's interface into the network. Once the connection has been established, the session layer can manage the dialog in an orderly manner, if the user has requested that service. [Ref. 5: p. 16-19]

6. Layer 6: Presentation Layer

This layer provides a host-to-host procedure that prescribes how data formatting and data transformation will be done. The function of the presentation layer is to

provide the user with certain useful but not always essential services. Among these services are cryptographic transformations, text compression, terminal handling, and file transfer. [Ref. 5: p. 386]

7. Layer 7: Application Layer

In principle there is little we can say about the content of the application layer, because each user determines what programs he will run and what protocols he will use. Furthermore, there are almost no national or international standard protocols for layer 7. [Ref. 5: p. 440]

C. SWITCHING TECHNOLOGY

Three different kinds of switching technology are used for data transmission in networks. Circuit switching is the most expensive because a circuit must be dedicated for a single message whenever one is exchanged. Message switching requires considerable computer memory, and it is not very economical. Packet switching is the cheapest and most efficient switching technique of the three. It does not require lengthy use of a circuit. Messages are broken into mutiple segments that can be forwarded in random sequence, reducing delay time and improving data flow performance. Figure 4 on page 11 illustrates event timing for the four kinds of switching technology. [Ref. 6: p. 200]

1. Circuit Switching

When a telephone call is placed, the switching equipment within the telephone system seeks out a physical "copper" path all the way from the initiator's telephone to the receiver's telephone. This technique is called circuit switching. Circuit switching requires an end-to-end connecting wire path between the calling parties. Once the path has been established, data transmission is delayed only by the propagation time for an electromagnetic signal. As a consequence of the established path, there is no danger of congestion; once the call has been put through, the user will never get a busy signal. [Ref. 5: p. 115]

2. Message Switching

Message switching makes better use of a network's bandwidth but allows messages to stack up in queue, causing delays. When message switching is used, no physical copper path is established in advance between sender and receiver. When the sender has a block of data to be sent, it is stored in the first switching office and then forwarded later, one hop at a time. Each block is received in its entirety, inspected for error, and then retransmitted. [Ref. 5: p. 115]

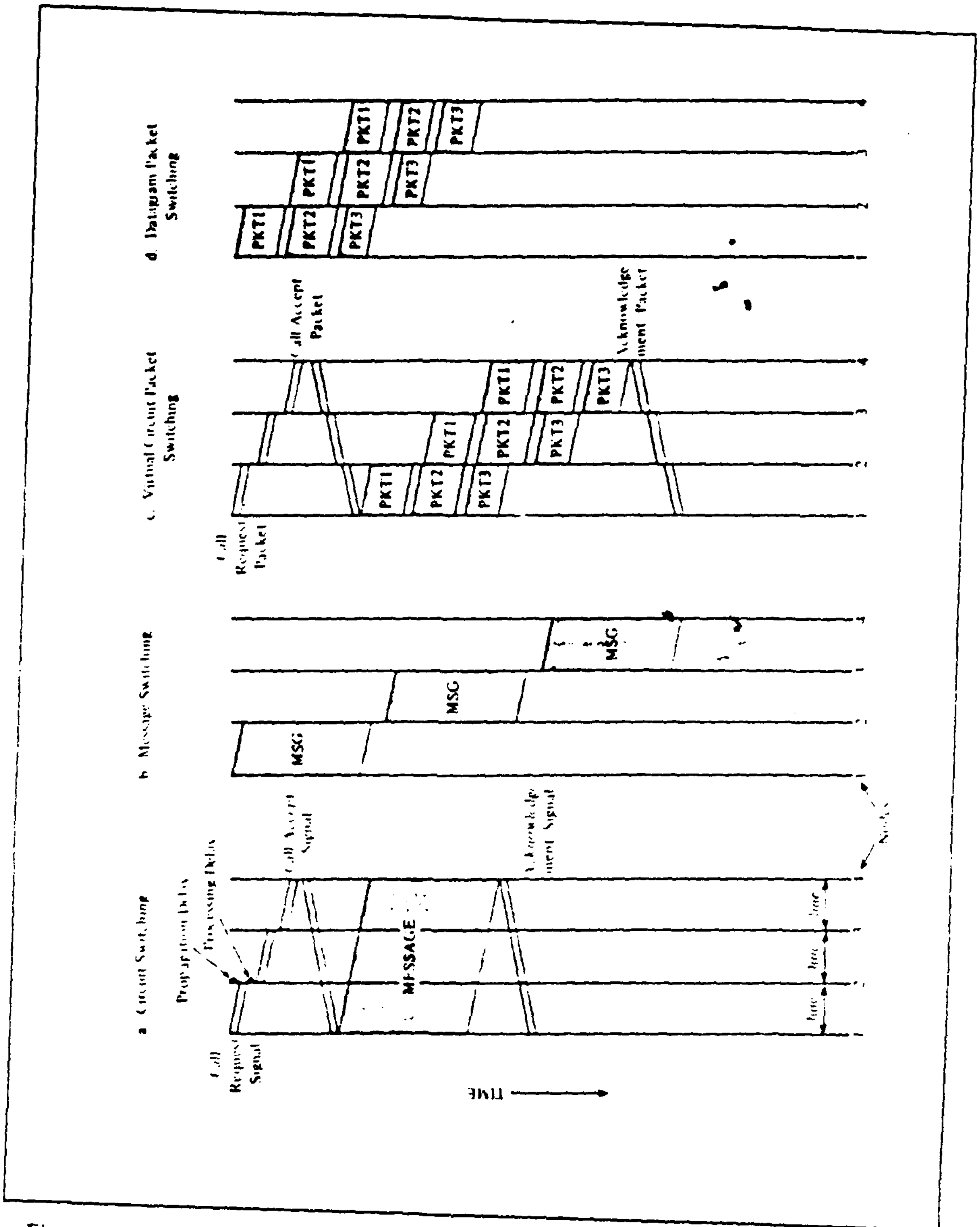


Figure 4. Four Switching Techniques for Data Transmission in Networks

3. Packet Switching

Packet switching represents an attempt to combine the advantages of message and circuit switching while minimizing the disadvantages of both. Packet switching is very much like message switching. The principal external difference is that the length of the units of data that may be presented to the network is limited in a packet-switched network. Another difference from message switching is that packets are typically not filed on a disk for transmittal to the next node. [Ref. 6: p. 197]

Packet switching networks place a tight upper limit on block size, allowing packets to be buffered in the packet switching node main memory instead of on disk. Thus packet switching networks are well suited to handling interactive traffic. The first packet of a multipacket message can be forwarded before the second one has fully arrived, reducing delay and improving throughput. [Ref. 5: p. 116]

With packet switching, nodes may be utilized by numerous packets from unrelated sources going to unrelated destinations, because circuits are never dedicated. When packet switching is used, it is straightforward for the packet switching nodes to provide speed and code conversion. They also can provide error correction to some extent. However, in some packet-switched networks, packets may be delivered in the wrong order to the destination. [Ref. 5: p. 117]

4. Packet Stream Technologies

There are two common approaches to transmitting entire messages over a packet-switched network. These are termed datagram and virtual circuit packet streams. In the datagram approach, each packet is treated independently, just as each message is treated independently in a message-switched network. The packets, each with the same destination address, do not all follow the same route. In the virtual circuit approach, a logical connection is established before any packets are sent. Thus the main characteristic of the virtual-circuit technique is that a route between stations is set up prior to data transfer. [Ref. 6: p. 198]

Most LANs use one of these packet switching stream technologies to exchange messages. The network uses some communication medium to connect the interfaces between various terminals. Access equipment controls the communication medium, allowing each transmission station to send messages in an assigned slot time. Stations must wait to send data until their assigned times.

D. TRANSMISSION MEDIA

A variety of technologies are available to implement a LAN's communication or transmission medium. These include:

1. Wire pairs and cables
2. Coaxial cable
3. Microwave circuits
4. Lightwaves and optical fibers
5. Satellite stations.

1. Wire Pairs and Cable

Wire pair is the oldest satisfactory electronic transmission technology. It consists of a pair of copper wires strung between poles, carrying one voice-grade channel that is used alternately by a number of subscribers on the network. One pair of wires can serve only two points at a given time. This type of facility usually is part of the analog public telephone network and can only be used for low-speed data traffic. Some wire pairs are used for purely digital transmission and can handle high-speed data rates. Transmission rates of 1.544 Mbps over twisted pairs are common for such digital transmissions. [Ref. 1: p. 66]

Wire pairs now have largely been replaced by other transmission media for voice communications. For data transmission over long distances, use of wire pairs becomes expensive, primarily because of the cost of copper and of labor for installlion. Wires are being replaced by microwave and satellite stations and by optical fibers. [Ref. 1: p. 66]

2. Coaxial Cable

A coaxial cable consists of a conductive cylinder with a central wire or solid core, held in place by an insulating material. A coaxial cable can transmit at a much higher frequency than can a wire pair, greatly increasing the transmission capacity. In addition, coaxial cables have very little distortion, cross talk, or signal loss and therefore are a more reliable medium for data transmission. Coaxial cable is commonly used to connect computers and terminals distributed among an organization's buildings on a single site. [Ref. 1: p. 66]

3. Microwave Circuits

More than half of the miles of circuits in the United States telephone system now are microwave circuits. Microwave systems use very high frequency radio waves. Because of their short wavelength, microwaves exhibit some of the characteristics of lightwaves; they travel in straight lines, can be reflected, and can be directed or focused

by special lenses. Microwaves are accurately beamed in line-of-sight transmission from one antenna tower to another 25 to 35 miles away. The spacing sometimes varies because of mountains or other physical obstructions. At each tower the weakened microwave signal is received, amplified, and retransmitted to the next antenna. Microwave circuits usually are not used for LANs. [Ref. 1: p. 66]

4. Lightwaves and Optical Fibers

Lightwaves and optical fibers are used as a transmission medium for both voice and data communications. The medium can carry high bandwith signals, yet it is very flexible and can be used to provide non-line-of-sight transmissions. This is especially important in urban areas. [Ref. 1: p. 66]

Optical fiber transmission has two significant advantages for data transmission. First, the transmitted signals are practically immune from noise and distortion, so that the medium is very reliable. Second, security can be ensured; the signal cannot be tapped without disturbing the medium itself. In addition, the data rate is very high and the medium is relatively low in cost. [Ref. 1: p. 66]

5. Satellite Stations

Communication satellites provide a special form of microwave relay transmission. The satellite is essentially a microwave antenna that has been placed in earth orbit. It can relay signals over longer distances than is possible with earth microwave stations because the curvature ofthe earth and physical obstacles block line-of-sight microwave transmission between land-based microwave towers. In addition to the satellites, a satellite communication system requires earth stations for initiation and receipt of transmission. Communication satellites are generally geostationary. That is, the satellite appears to be stationary to the earth ground stations. A satellite receives microwave signals in a given frequency band, amplifies them, and retransmits them at a different frequency. [Ref. 1: p. 67]

Satellite channels will be increasingly used for long-distance, high-volume data transmission. Use of rooftop antennas at an organization's various locations could avoid the need to use other common carrier long-distance facilities. However, satellite transmissions are not used for LANs, at present. [Ref. 1: p. 67]

E. TRANSMISSION PROTOCOLS

Data link control protocols are the rules for transfering data and control information over a data communications link to remote stations. It is useful to classify such protocols into two basic groups: asynchronous protocols and synchronous protocols

[Ref. 2: p. 112]. It must be realized that such a single protocol is in fact composed of several subprotocols.

An asynchronous protocol is one in which data are transferred at nonuniform rates. The beginning of each character is marked by a start bit and the end of each character by a stop bit. The use of start and stop bits associated with each character is not efficient, and such protocols are not useful for high data rate applications. [Ref. 2: p. 112]

Synchronization refers to the technique used so that the receiving and transmitting stations can maintain synchronous clocks. The transmission of a special synchronization idle character is one such technique. [Ref. 2: p. 114]

Synchronous protocols provide for the transfer of data at a fixed rate with the transmitter and receiver operating in synchronization. Synchronous modems are typically used so that a clock signal is transmitted along with the data stream to ensure that the transmitter and receiver stay in synchronization (see Figure 5 on page 16).

For two devices linked by a transmission medium to exchange synchronous data, a high degree of cooperation is required. Typically, data messages are transmitted one bit at a time over a communication medium transmitter. The receiver must recognize the beginning and end of a block of bits. [Ref. 6: p. 100]

Synchronous protocols may be classified into three types, depending on the *message-framing format* used:

1. Character-oriented protocols
2. Bit-oriented protocols
3. Byte-oriented protocols.

Character-oriented protocols use a special character to designate the beginning and end of the message portion. Bit-oriented protocols utilize a special flag character to identify the message. Byte-oriented protocols utilize a header that includes a "count" parameter which indicates the number of data characters in the message. [Ref. 2: p. 114]

F. COMMUNICATION MODES

Two kinds of communication modes are used for LANs. These are called fullduplex and halfduplex. Under fullduplex communications, data are transmitted in two directions at the same time. A user on one terminal can send data at the same time as the person he is communicating with the sending data. When halfduplex transmission is used, data are being sent in only one direction at a time. One user sends his data, then the other person sends his data.

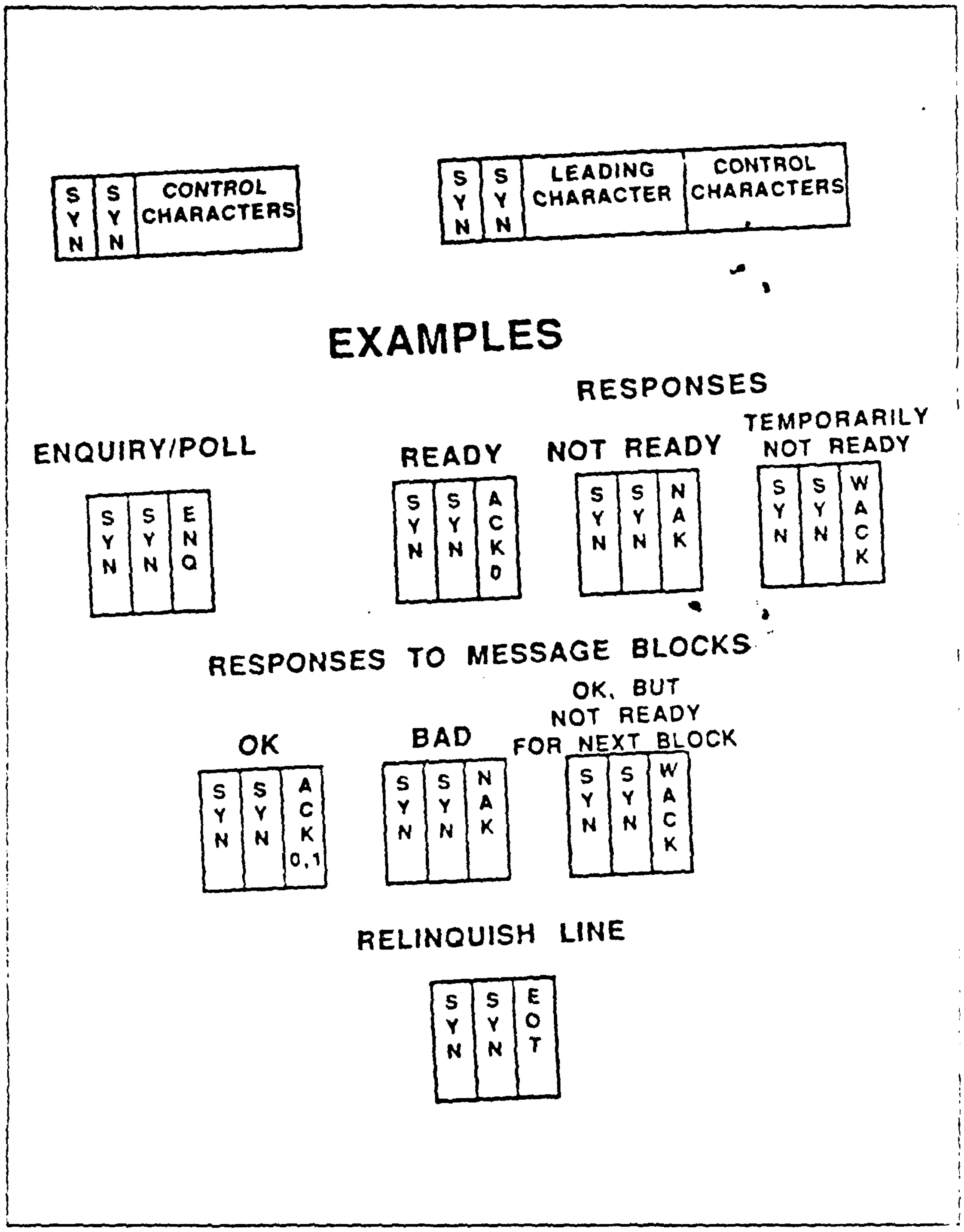


Figure 5. Synchronous Transmission of Data

G. MODEM

A modem is a device used to make connections between a given computer and a telephone line. A digital signal is converted to an analog signal by a modulator. The analog signal then is converted back to a digital signal by a demodulator, after transmission through the lines. The word modem comes from the terms modulator and demodulator. There are two kinds of modems. External modems are peripheral devices that are not permanently attached to the computer. Internal modems are installed inside the computer, and become part of a given computer system.

H. LAN TOPOLOGIES

Four LAN topologies that are generally considered feasible. These are referred to as mesh, star, bus, and ring networks.

1. Mesh Topology

In a mesh network, each device has a point-to-point link with every other device, as illustrated in Figure 6 on page 18. This is referred to a fully connected or mesh topology [Ref. 6: p. 35]. Most networks employ a mesh configuration either by itself or in combination with one or more of the other configurations, thereby forming a hybrid configuration [Ref. 7: p. 14].

a. Advantages

- The mesh configuration has low response time and is robust against node or link failure.
- This topology is well suited and commonly used for long-haul packet-switched networks [Ref. 8: p. 33].

b. Disadvantages

- Mesh topology is very complex.
- This topology is extremely expensive, relative to the bus and ring types, without a proportionate advantage in efficiency [Ref. 7: p. 14].

2. Star Topology

In star network, each network node accepting and delivering user traffic is connected to a single central node through which all traffic must pass (see Figure 7 on page 19) [Ref. 7: p. 14]. The central node acts as the system control and has separate communication lines to all other nodes. Normal telephone systems employ a star topology. [Ref. 7: p. 14]

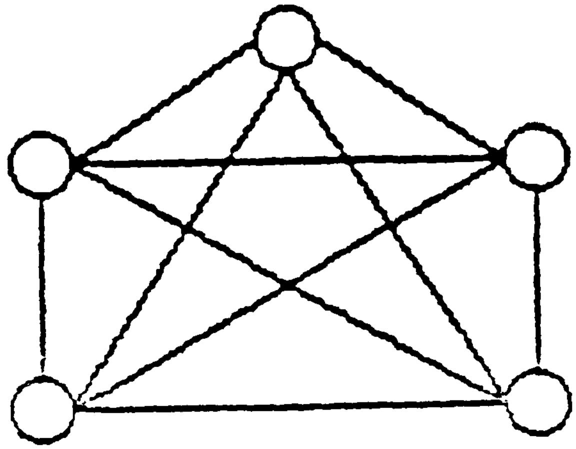


Figure 6. Mesh Topology for LANs

a. Advantage

- Point-to-point lines connect the central and outlying nodes, eliminating the need for the complex link and control requirements of other topologies, and allowing simple and usually low cost connections to the network through the central node. [Ref. 8: p. 35]

a. Disadvantages

- This topology is extremely expensive relative to the bus and ring (without a proportionate advantage in efficiency) because it uses dedicated lines to connect each node to the network. [Ref. 7: p. 14]
- A basic problem with the star configuration is that if a node or link fails, computers on one side of the failure are unable to communicate with computers on the other side of the failure. [Ref. 9: p. 688]

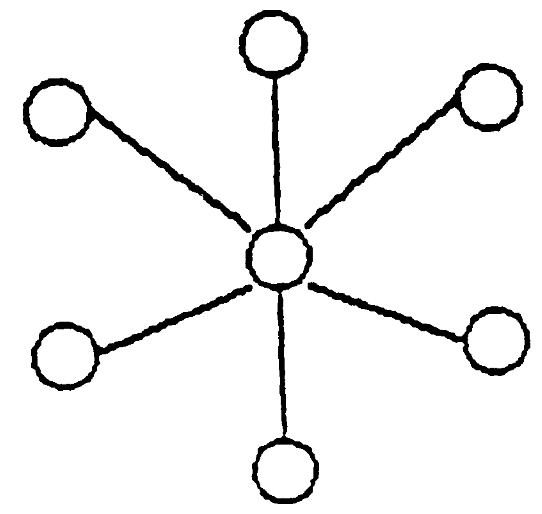


Figure 7. Star Topology for LANs

3. Bus Topology

When all network nodes connect to a single transmission medium they form what is termed bus topology (see Figure 8 on page 20). Each node has a unique address used to identify it. The bus is typically multiplexed allowing information to be transmitted in short, high-speed bursts. [Ref. 7: p. 14]

a. Advantages

- Bus nodes share a single physical channel via cable taps or connectors.
- Messages placed on the bus are broadcast out to all nodes.
- Unlike nodes in a ring, bus nodes do not have to repeat and forward messages intended for other nodes. As a result, there is none of the delay and overhead asso-

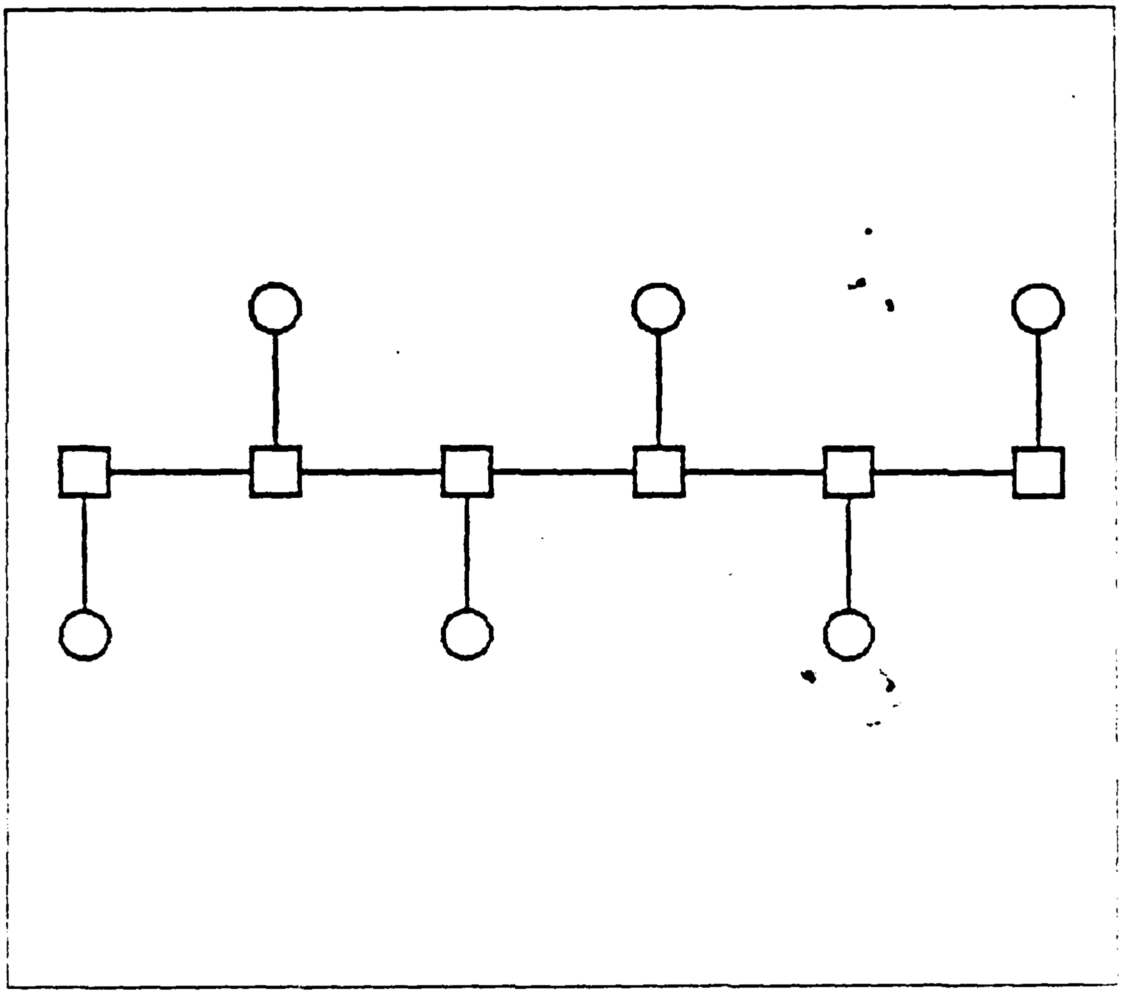


Figure 8. Bus Topology for LANs

ciated with retransmitting messages at each intervening node, and nodes are relieved of network control responsibility at this level.

- Bus networks are easily configured and expanded in most physical layouts, for instance a room, building, or building complex. This feature alone is often a major reason in choosing the bus topology for a local network. [Ref. 8: p. 38]

a. Disadvantage

- In some bus topologies, if nodes are physically too distant from each other, collision of two messages may not be detected.

4. Ring Topology

A ring network consists of nodes each of which has connections only to the node on each side of itself, such that a complete circle is constructed (see Figure 9 on

page 22). Data must pass through all nodes between the sender and receiver. [Ref. 5: p. 35]

a. Advantage

- Ring nodes can be less complex than the routing nodes in an mesh topology, since message routes are determined by the topology--messages automatically travel to the next node on the ring.

b. Disadvantages

- Rings must be physically arranged so that they are fully connected. Lines have to be placed between any new node and its two adjacent nodes each time an addition is made. Thus, it is often difficult to prewire a building for ring networks in anticipation of nodes to be added in the future.
- Failure of a node or an active component adding a new node, or any other break in the ring topology will most always cause the network to stop functioning. [Ref. 8: p. 36-37]

I. NETWORK ACCESS TECHNIQUES

Terminals connected into a the network must use some method of accessing that network. Different access methods are available and have different functions. Two basic access methods are centralized control and distributed control. With centralized control, one device controls access for the others. Distributed control allows individual devices to control their own access. Several types of network access methods currently are used for LANs. These include time division multiple access (TDMA), frequency division multiple access (FDMA), carrier sense multiple access (CSMA), token passing on ring networks, and token passing on bus networks.

1. Time Division Multiple Access

Packet switching TDMA allows each user, in sequence, to transmit a single packet 1000 bits in size. Each packet is initially stored in the computer's buffer. When the network's concentrator-commutator selects a particular buffer, the bits are read out of the buffer and on to the common channel at the network's bit rate. [Ref. 9: p. 696]

TDMA systems are very efficient if the users have a continual need to transmit. However if users' transmission needs vary from time to time or if users rarely transmit, then TDMA becomes inefficient. This is because a user pays for the time slot, even when he fails to transmit. His time slot is wasted. During this wasted time an additonal user could have been admitted to the network. However, when the data are digital, TDMA is more "natural"; as technology improves, more systems are converting to TDMA. [Ref. 9: p. 696]

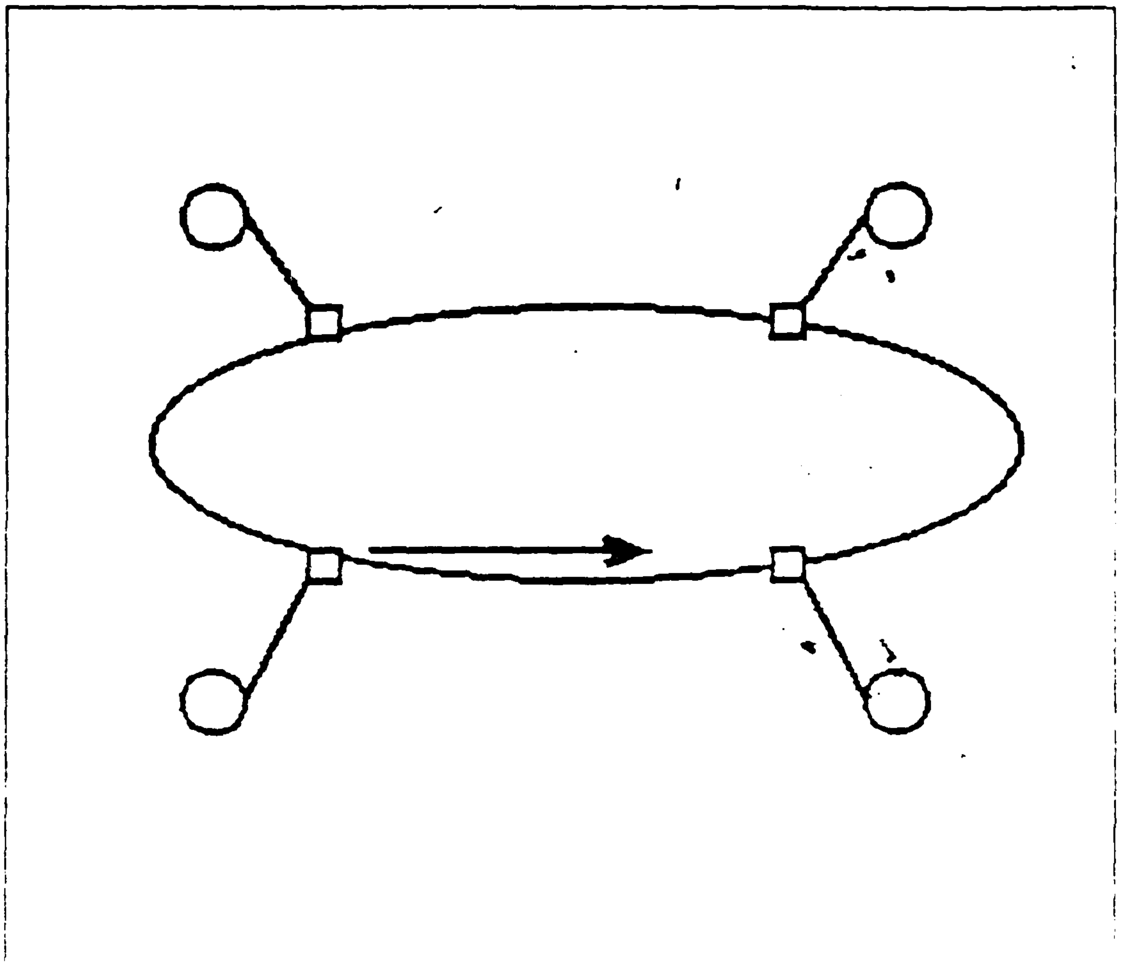


Figure 9. Ring Topology for LANs

2. Frequency Division Multiple Access

Under FDMA systems, each user can transmit all of the time, but each must use only a portion of the total bandwith. [Ref. 9: p. 698]

FDMA is a more popular technique than TDMA due to technology problems arising from building very high-speed circuits required by TDMA. As is the case for TDMA, FDMA is efficient as long as each user requires the use of the network a large percentage of the time. If such is not the case, available bandwith is being wasted since other users could have transmitted on these bandwiths. Using FDMA these extra users were denied access to the network. [Ref. 9: p. 698]

3. Carrier Sense Multiple Access

In a CSMA system, each user tunes a receiver to the common carrier frequency employed by all users. Before transmitting, a user (or his computer) will listen to determine if any of the other users are transmitting; if no other user is transmitting, the computer will transmit the packet. All potential transmitting users generally are geographically closely clustered as are all potential receiving users. Propagation delay between transmitting users then can be ignored and there will be no data collisions. [Ref. 9: p. 704] If all users are not close to one another, data collisions can become a serious problem.

The ability to detect collisions and shut down the transmitter promptly is an important feature in minimizing the time on the channel lost to collisions. Some CSMA systems have this ability, and are called CSMA with collision detection (CMSA/CD). The general requirement is that, while transmitting, a controller must recognize that another station is also transmitting. There are two approaches:

- Collision detection in the transmission system. It is usually possible for the transmission system itself to recognize a collision. This allows any medium-dependent technique to be used, and is usually implemented by comparing the injected signal with the received signal. Comparing the transmitted and received signals is best done in the transceiver where there is a known relationship between the two signals. It is the controller, however, which needs to know that a collision is taking place.
- Collision detection in the controller. Alternatively, the controller itself can recognize a collision by comparing the transmitted signal with the received signal, or unilaterally attempting to recognize collisions, since they often appear as phase violations. [Ref. 10: p. 18]

4. Token Passing Access

A token is a predetermined bit pattern that travels through the network from station to station. Possession of the token enables a station to transmit signals to the network communication channel. If that station has nothing to communicate, the token is passed to the next station.

Token passing techniques differ with network topology. In a ring network, consecutive nodes must be physically adjacent to one another, with the token passed between the nodes through the physical communications ring. In a bus network, a "logical ring" may be created, and the consecutive nodes on the ring need not be physically adjacent. [Ref. 11: p. 58]

III. ARCHITECTURE AND DESIGN OF LANS

Local networks use simple protocols to transmit messages. Long distance networks use more complex protocols to transfer and receive packets. The kinds of computers on LANs usually use less complex protocols than those on wide area networks (WAN) when LANs and WANs are interconnected. This chapter discusses how current WANs and LANs can work together.

A. INTERCONNECTION ISSUES

As the capability of software on LANs grows to handle document management, file transfer, electronic mail, etc, the need to expand into wide area data communication also increases. It is necessary to consider WAN and LAN interconnection issues before planning and designing new LANs. When communication is desired among different machines the software development effort will be difficult. This is especially true when one or more local networks is interconnected with one or more long-distance networks because different vendors use different formats, data flow, error control, etc., for exchange of data.

The differences between local and long-distance networks is summarized in Table 1 on page 25, showing how these can lead to major interconnection issues. [Ref. 3: p. 17]

1. Interconnection Requirements

Three capabilities are necessary to interconnect computers into a network. These are network access, network services, and protocol functions. First, network access is achieved via frontend processor hardware in conjunction with access lines and mainframe-to-packet switch node protocol.

Second, basic network services must be provided. These include virtual circuit service for interactive processing and other operations that require reliable, sequenced end-to-end message delivery, and datagram service for operations which involve the transmission of independent messages. Datagram service, implemented in the internet protocol (IP) and operating in the network layer, supports transmission control protocol (TCP), operating in the transport layer, to provide a virtual circuit service. Datagram service is used to obtain efficient bandwidth utilization and flexibility. Messages can be transmitted as independent packets without being constrained to follow a single path or required follow one another in sequence. TCP sequences the messages and provides reliable end-to-end delivery.

Table 1. COMPARISION OF LOCAL AND LONG-DISTANCE NETWORK CHARACTERISTICS

CHARACTERISTIC	LOCAL NETWORK	LONG-DISTANCE NETWORK
Typical Bandwith	10 million bits per second.	56,000 bits per second.
Acknowledgment	One message acknowledged at a time.	N messages acknowledged at a time.
Message Size and Format	Small (simple header). No need to divide message into packets.	Large (complex header). Need to divide message into packets.
Network Control	Minimum requirement due to small number of links and nodes and simple topology.	
Flow/congestion Control	Minimum due to high bandwidth and simple topology.	Extensive due to low bandwidth and complex topology.
Error Rate	Relatively low. Operated in benign environment.	Relatively high. Operate in noisy environment of telephone network.
Message Sequence and Delivery	Minimum problem due to simple topology (e.g., bus or ring).	Major problem due to complex topology (e.g., mesh).
Standard Architecture	Usually only two or three bottom layers provided.	Frequent use of all or many ISO layers.
Routing	None required due to simple topology.	Major problem due to complex topology.
Delay Time	Small due to short distance and medium (e.g., coaxial cable).	Large due to distance and medium (e.g., satellite).
Addressing	Simple intra-network communication due to simple topology. Complex inter-network communication due to the use of long-distance networks.	Complex because of many nodes and links.

Third, protocol functions are necessary to support communications among various computers linked in the network. Due to the great differences between local and long-distance network characteristics, protocol requirements may differ significantly between the two types. [Ref. 3: p. 21]

To maximize compatibility and minimize software complexity, protocols for LANs and WANs should be selected to match as closely as possible, consistent with satisfying the requirements of vastly different communications environments. Protocol matching is necessary for satisfactory performance, especially for inter-local network services and long-distance networks when optimization of intra-local network performance is desired. This is accomplished by using only those layers and protocols that are compatible with and can take advantage of the characteristics of local networks. Of course, the user organization must be willing to pay the relatively high software cost of this tailored approach. [Ref. 3: p. 24]

2. Bridge Routing Concepts

A bridge is a computer that always connects exactly two subnetworks. Its job is to pick packets from one subnetwork, check their destinations and security levels, and send them to the other subnetwork. To prevent congestion, bridges must operate at a speed fast enough to handle a reasonable load of traffic from one subnetwork to another. [Ref. 5: p. 382]

Since a subnetwork may have a number of bridges attached to it and a bridge connects two subnetworks to each other, the possibility exists for multiple paths from a source to a destination at a LAN site. In such situations, a bridge might be required to decide on which path to transmit a packet, based on the dynamics of the load on the two subnetworks. While this may be desirable in some situations, static routing is recommended for simplicity. Suitable restrictions are needed to define only one logical path between each pair of source and destination addresses on a given LAN. Such a unique path from a source to a destination can be ensured by requiring that only one bridge on a subnetwork can receive a packet destined for a host on a different subnetwork. [Ref. 12: p. 25]

Each bridge will read the destination subnetwork number in the header part of each packet and pick a packet for transmission into other subnetwork if the bridge provides logical connectivity to the destination subnetwork. This means that a bridge must store information about all the destination subnetworks that lie on logical paths through

it. One convenient way of storing this information in a bridge is in the form of row vectors. [Ref. 12: p. 25]

3. Gateway Routing Concepts

As more and more networks come into existence the need to interconnect them arises. Interconnection can be accomplished by inserting a gateway computer between pairs or larger groups of networks. A gateway is a processor connecting two networks. Its primary function is to relay data between networks using an internetwork protocol. Typically, the gateway operates as a host. When networks with different maximum packet sizes are interconnected, there is a need to fragment large packets and then reassemble the pieces later. Two approaches to packet-switched internetworking have been tried: concatenated virtual circuits and datagrams. Depending on the details of the internetwork strategy adopted, the transport layer may be considerably or only marginally affected by the requirements of internetworking. [Ref. 5: p. 382]

A gateway node provides an interface between a LAN and a WAN for establishing long-distance communications between nodes within the LAN and nodes that are within other LANs or that are accessible directly on the WAN. Wide-area networks include private and commercial packet-switched networks, satellite links, leased lines, and other terrestrial links. They generally operate at lower transmission rates than most LANs, usually in the kilobits per second transmission range. A gateway can perform the necessary address translations as well as provide the speed and protocol conversions that are required to interface the LAN to a WAN. Similar functions are required to interface a host computer to a token ring via a ring-to-channel gateway. There are also applications where a gateway can be used as an intermediate node between a token-ring LAN and a node on a network using CSMA/CD topology. [Ref. 13 : p. 24]

B. COMPARISON OF APPROACHES

Four general architectural approaches have been proposed for LANs that will interconnect with WANs. In addition to the OSI model (dissussed earlier), they are DoD protocol architecture, systems network architecture, and Digital network architecture. These are discussed below.

1. DoD Protocol Architecture

DoD protocol architecture (DPA) is like the OSI architecture in that it deals with communications among heterogeneous computers. Both are based on the concept of protocol and have many similarities. However, there are philosophical and practical

differences between the OSI model and the DPA. The DPA organizes protocols into four layers. [Ref. 6: p. 398]

Network Layer: Protocols at this layer are between a communications node and an attached host or its logical equivalent. A function of all these protocols is to route data between hosts attached to the same network. Other services that may be provided are flow control and error control between hosts. [Ref. 6: p. 398]

Internet Layer: The internet layer consists of the procedures required to allow data to traverse multiple networks between hosts. Thus it must provide a routing function. This protocol is usually implementd within hosts and gateways. [Ref. 6: p. 398]

Host-Host Layer: A protocol entity at this level may provide a logical connection between higher-level entities. Indeed, it is at this level that explicit connections make the most sense, with a logical connection being one used to exchange data between the ultimate endpoints. Other possible services include error and flow control and the ability to deal with control signals not associated with a logical data connection. Four general types of protocols usually are needed at this level: a reliable connection-oriented data protocol, a datagram protocol, a speech protocol, and a real-time data protocol. [Ref. 6: p. 398]

Processor/Application Layer: This layer contains protocols for resource sharing and remote access [Ref. 6: p. 399].

2. Systems Network Architecture

Systems network architecture (SNA) consists of five layers. These are called:

Data Link Control: SNA does not address directly what OSI refers to as the physical layer, but only implies it. Hence the bottom layer of SNA is data link control. [Ref. 6: p. 399]

Path Control: The path control layer creates a logical channel between endpoints, referred to as network addressable units (NAUs). An application-level entity capable of being addressed and of exchanging data with other entities, the path control layer has routing and flow control as its key functions. [Ref. 6: p. 400] Thus the path control layer is similar to the ISO network layer and is responsible for the following functions.

- Static routing functions: routes are chosen from fixed tables which are determined at transmission time. Each possible source-destination combination has a list of alternate routes to be chosen from, depending on class of service selected.
- Supporting three priority levels for network traffic.

- Controlling the rate of data flow for all network traffic on each path. [Ref. 14: p. 7-3]

Transmission Control: This is next higher layer of SNA: it corresponds roughly to layer 4 of the OSI model. The transmission control layer is responsible for establishing, maintaining, and terminating SNA sessions. A session, which corresponds to OSI's transport connection, is a logical relationship between endpoints (NAUs). The transmission control layer can establish a session in response to a request from the next higher layer, from an application process, or for its own control purposes. [Ref. 6: p. 401]

Data Flow Control: The data flow control layer is end-user oriented and corresponds to OSI's layer 5 (session layer). This layer is responsible for providing session-related services that are visible and of interest to end-user processes and terminals. [Ref. 6: p. 402] The principal functions are:

- Controlling the send-receive state of a session, which can operate in half duplex flip-flop, half duplex connection, or full duplex mode.
- Controlling arrival of messages to a process, assuring complete message integrity. [Ref. 14: p. 7-4]

Function Management Data Services: The top layer of the SNA architecture is the function management data (FMD) services layer. It consists of a collection of functions and services provided to the end user. It encompasses OSI's layer 6 and has some elements of layer 7. FMD consists of two main components: session presentation services and session network services. [Ref. 6: p. 402] The session presentation services component is essentially like OSI's presentation layer, and includes the following services:

- Text compression and compaction.
- Terminal data streams, intermixing data with control characters, reading, writing, erasing, intensity control, etc.
- File management, such as creating, destroying, or updating remote files. [Ref. 14: p. 7-4]

3. Ditigal Network Architecture

Digital network architecture (DNA) has been developed by Digital Equipment, Inc. There is no session layer in DNA. However, DNA plans to add a session layer as soon as the ISO standardizes one. At present it is composed of four layers:

Physical and Data Link Layers: DNA recognizes the concept of a physical layer and allows a variety of hardware interfaces. [Ref. 6: p. 404]

Transport Layer: The transport layer corresponds to the network layer of OSI. The transport layer provides a datagram service and performs the following functions:

- Routing
- Congestion control
- Packet lifetime control
- Transport initialization. [Ref. 6: p. 404]

Network Services Layer: This layer performs the functions of the OSI transport layer, using Digital Equipment's proprietary network services protocol (NSP), which will be replaced in the future by a proposed OSI transport protocol. This layer deals with the problems caused by an unreliable network, such as discarded, duplicated, or out-of-sequence packets. In an attempt to provide reliable transport service to the application layer, the NSP uses such techniques as three-way handshaking. [Ref. 6: p. 405]

Network Application Layer: The network application layer contains the highest system-supplied functions in DNA and provides services such as remote file access, file transfer, and remote system load. The most prominent module assigned to this layer is the data access protocol which allows remote file access and manipulation and includes a negotiation process to determine whether or not the two systems involved in a data exchange use the same file format. If not, one or both systems must convert to the defined network standard format. This layer corresponds roughly to OSI's layer 6 and part of layer 7. [Ref. 6: p. 405]

C. PROTOCOLS AND STANDARDS

1. Protocol Specification and Verification

Communication protocols play an important role in computer networks and distributed systems. The increasing variety and complexity of such protocols demand more powerful techniques to produce successful systems. A great deal of confusion surrounds the words "specification" and "verification" as they apply to computer communication protocols. [Ref. 15: p. 467] In the context of a layered model of protocols, these concepts can be defined as:

Specification: Any information that helps describe an object. Because a specification is abstract, there are many ways in which an object can be designed to meet its specification. A specification should state all the requirements that an object must satisfy. [Ref. 15: p. 468]

Verification: A demonstration that an object or system has certain properties or behaves in a certain way. This requires a clear statement of the properties or behavior to be verified. Verification is simply a demonstration that an object meets its specifications. [Ref. 15: p. 468]

Protocol specification requires a clear definition of both the services to be provided by a given protocol layer and the modules within the la r that cooperate to provide the service. Design verification then consists of showing that the interaction of protocol modules is indeed adequate to provide the specified services. Implementation verification consists of showing that the protocol modules satisfy their protocol specifications. A useful subset of design verification is verfication of "general properties" such as deadlock, looping, and completeness. For most protocols, these properties may be checked without requiring any particular service specification. [Ref. 15: p. 472]

One example of protocol verification is the verification of call establishment in the International Committee on Telegraphy and Telephone (CCITT) X.21 protocol. The protocol has been modeled with a state transition model and analyzed with a form of reachability analysis. During verification the analysis checked for the general correctness properties of completeness and deadlock, and uncovered a number of completness errors. [Ref. 15: p. 472]

Virtual circuit establishment in the CCITT X.25 protocol has been modeled and analyzed with a manual reachability analysis. The analysis showed that the CCITT specification was ambiguous, and that several cycles with no useful progress could persist if the protocol once entered certain unsynchronized states. [Ref. 15: p. 472]

Connection establishment in the transport protocol for the DoD Arpanet network has been partially modeled with a hybrid state transition model and validated with a manual reachability analysis. An automated reachability analysis was also used on a simplified model and revealed both an error in sequence number handling and incorrect modeling of the transmission medium. [Ref. 15: p. 472]

2. Standards

The standardization of local area networks is an activity that serves the interests of both network users and the industry that provides LAN products. National and international standards for the token ring have been developed as part of the family of LAN standards developed primarily by the Institute of Electrical and Electronics Engineers (IEEE) in the United States and the European Computer Manufacturers Association (ECMA) in Europe. The standards produced by the IEEE and ECMA become

international standards if they are introduced by member countries to the ISO, headquartered in Geneva, Switzerland, and accepted by that body. [Ref. 13: p. 19]

LAN standards apply to the data link and physical layers of the OSI reference model, with consideration of the network layer only in terms of the service that LANs provide to the network layer as a user of the data link layer. The data link layer is divided into two sublayers for LANs: logical link control (LLC) and medium access control (MAC) layers. Together they perform the duties of the data link layer, namely frame exchange between peer data link layer entities. [Ref. 13: p. 20]

The token-ring standard contains the formats and protocols for the MAC and also the associated physical layer specifications. Formats are given for the token, a generic frame, and the information field of ring management frames for the selection of an active monitor for duplicate address detection. The protocols include normal ring operation, selection of an active monitor, and numerous ring recovery procedures. The protocols are contained in an operational finite-state machine, a standby monitor finite-state machine, and an active monitor finite-state machine. [Ref. 13: p. 21]

3. Architectures

All LANs basically provide a communications subsystem for the purpose of transporting data between nodes on the network. The communications subsystem itself consists of some kind of communications medium such as coaxial cable or twisted-pair wires, arranged typically in a bus or ring topology, to which devices of various types are connected by means of network access units [Ref. 10: p. 88]. The most commonly-used LAN architectures are Ethernet and token ring.

4. Ethernet Architecture and Protocols

Ethernet is a multi-access, packet-switched communications system for carrying digital data among locally distributed computing systems. The shared communications channel in an Ethernet is a passive broadcast medium with no central control; packet address recognition in each station is used to take packets from the channel. Access to the channel by stations wishing to transmit is coordinated in a distributed fashion by the stations themselves, using a statistical arbitration scheme. [Ref. 10: p. 2]

One of the primary goals of the Ethernet specification is compatibility, providing enough information for different manufacturers to build widely differing machines in such a way that they can directly communicate with one another. There are many levels of protocols, such as transport and file transfer, which must also be agreed upon and implemented in order to provide useful services. The design of any LAN must be

considered in the context of a distributed system architecture, viewing the LAN as one component in an internetwork system that provides communications services to many diverse devices connected to different networks. [Ref. 10: p. 3]

The general Ethernet approach uses a shared communications channel managed through a distributed control topology known as carrier sense multiple access with collision detection (CSMA/CD), discussed briefly in Chapter II. With this approach, there is no central controller managing access to the channel, and there is no fixed pre-allocation of time slots or fixed sharing of frequency bands. A station wishing to transmit requests the use of the common shared communications channel until it acquires the channel; once the channel is acquired the station uses it to transmit a packet. [Ref. 10: p. 4]

The CSMA/CD topology is used in networks which utilize a common transmission media, e.g., bus topology. Each node connected to the common medium contends for access or control of the medium in a fully decentralized manner. Each packet carries its own set of overhead information, required for transmission. However, there is no transmission overhead when all nodes are idle. This is ideal for a light-traffic system where the ratio of overhead time to total utilized time is approximately constant. But when more and more traffic is directed to the transmission medium, collisions of packets from different nodes become common. The system spends significant portion of time to handling collisions and thus utilization of the medium degrades rapidly. [Ref. 16: p. III-33]

In a correctly functioning system, data collision may occur only within a short time interval following the start of transmission, since after this interval all stations will detect carrier use and defer transmission. The time interval is called the collision window or the collision interval, and is a function of the end-to-end propagation delay. If no collisions occur during this time, a transmitter has acquired the Ethernet and continues transmission of the packet; however collision monitoring must still be done in case a malfunctioning station begins to transmit. If a station detects data collision, the transmission of the rest of the packet is immediately aborted. Each transmitter involved in the collision then schedules its packet for retransmission at some later time. [Ref. 10: p. 4]

The Ethernet is intended primarily for use in office automation, distributed data processing, terminal access, and other situations requiring economical connection to a local communication medium carrying bursty traffic at high peak data rates. Experience

with Ethernet systems that support electronic mail, distributed filing, calendar system, and other applications has confirmed the usefulness of this approach. [Ref. 10: p. 30]

Two versions of Ethernet network architecture have been developed: an experimental version and a commercial one. The experimental Ethernet is characterized by a 3 Mbit/sec data rate and allows interconnection of up to 256 computers; the commercial version provides a data rate of 10 Mbit/sec and can connect up to 1024 computers. [Ref. 10: p. 170-174]

The Xerox coporation has developed a communications architecture centered on Ethernet and on the interface to such a network. This architecture is depicted in Figure 10 on page 35. [Ref. 10: p. 170-174]

Level 0 of this architecture consists of a number of network drivers which provide access to distinct data communications media and may implement different communications protocols.

Level 1 consists of the Internetwork Datagram Protocol. This level supports a uniform access interface to the various data communications media provided by level 0. Level 1 provides a process-to-process internetwork datagram service; it defines the format of the internet packet and the rules for its delivery as a datagram across mutiople networks.

Level 2 consists of a number of protocols which use the level 1 service to provide interprocess communications. These protocols include a sequenced packet protocol, an error protocol, a packet exchange protocol, and a routing information protocol.

Level 3 consists of protocols for the control and manipulation of resources, e.g., file servers, print servers, etc. Courier is a remote procedure call protocol; it implements the abstraction of procedure calls between computers connected by a data communications network and between programs written in different languages. Courier is based on the exchange of service requests and response messages between client and server processes distributed over a network. [Ref. 10: p. 170-174]

5. Token Ring Architecture and Protocols

Token passing on ring networks has been discussed in Chapter II. A token ring operates using one of three methods. In the simplest (and most inefficient) method, a station waits for all transmitted bits to travel around the ring and be removed before the token is forwarded. [Ref. 13: p. 12]

With the second method, the station forwards the token after its transmission is complete and the header of the first packet has returned. This scheme still provides

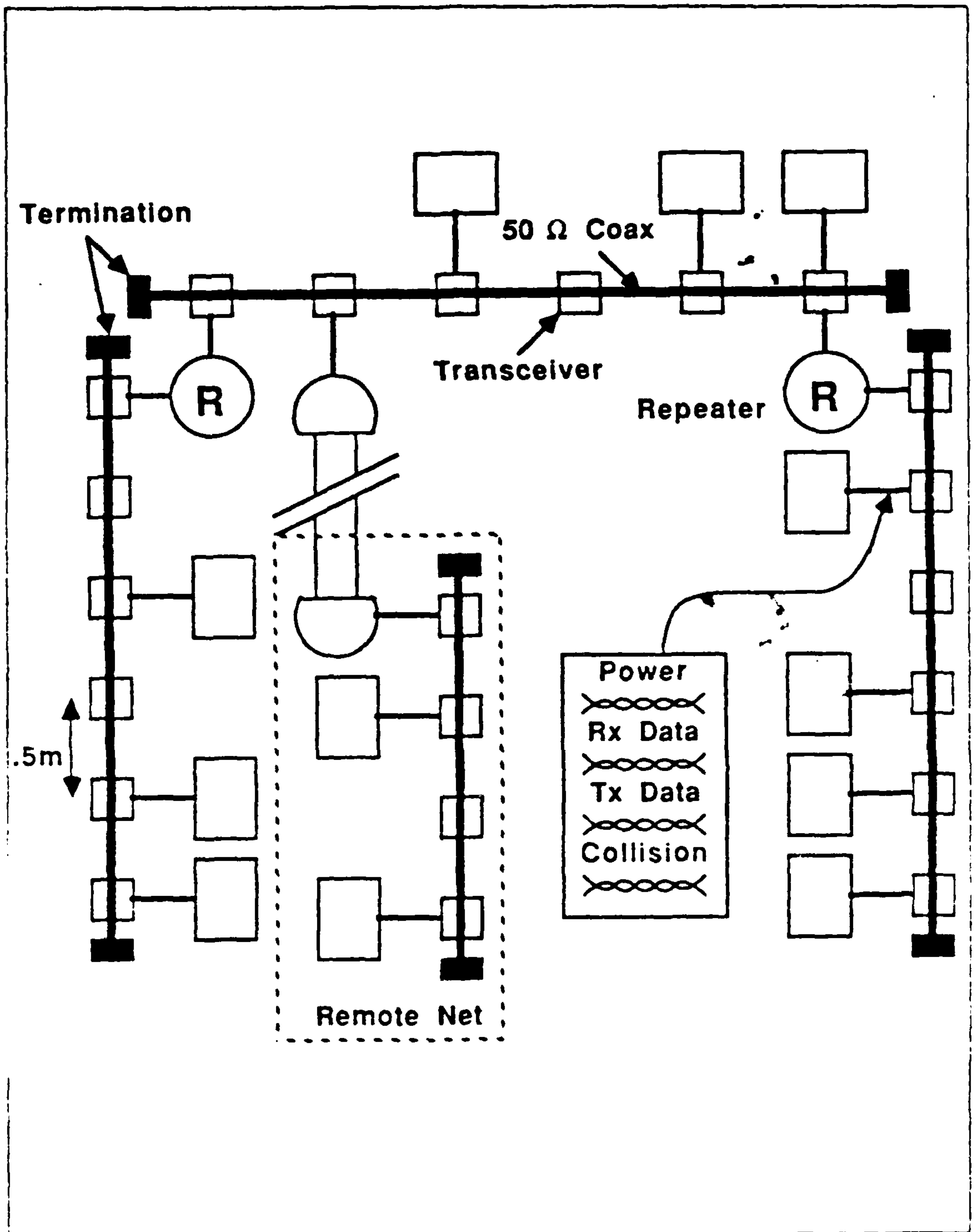


Figure 10. Xerox Ethernet Architecture

for a fairly simple removal of packets. It also allows the next station on the ring to begin transmission sooner than in the first method. [Ref. 13: p. 12]

For the third method, a station can also forward the token as soon as its transmission is complete, even though none of the transmitted data has returned yet. This is the most efficient technique, but increases the complexity of removing packets from the ring. [Ref. 13: p. 12]

The three methods are affected approximately equally if the number of stations, the total system cable length or the channel capacity is increased, or if the mean packet size is decreased. However the third method maintains its efficiency over a much wider range of system parameters than the first two methods. [Ref. 12: p. 52]

Instantaneous utilization of the system can vary considerably depending on the number of active stations and the characteristics of the traffic introduced onto the ring. As in any similar queueing system design, average system utilization should be maintained at a relatively low value. This allows the system to handle widely varying traffic conditions without significantly impacting the response time that is offered to any using station. [Ref. 13: p. 12]

Based on the networking structure as defined by the OSI reference model, the protocols for token ring LANs are representative of those used for the lower two layers: the data link layer and the physical layer. [Ref. 13: p. 12]

Logical link control functions are common across all multiple access control methods. Token-ring protocols provide the mechanisms for achieving the high degree of connectivity for logical nodes attached to the LAN. A station is the physical embodiment of the technology that implements the communication protocols of the data link layer in conjunction with the physical layer. Each station attached to a LAN can support multiple logical links for communication over the network, as well as multiple logical node devices. Furthermore, a single logical node may interface to the LAN through multiple logical links, supported by one or more stations. [Ref. 13: p. 12-13]

Multiple access control functions associated with token rings employ unique control fields that are not used with other types of access mechanisms. The sequential ordering of stations on the ring allows for each station to convey information to downstream stations by modifying the state of the bits in these fields. Being outside the coverage of the frame check sequence, the detection of data transmission errors is not impacted. Functions derived directly from these control bits include the basic access

mechanisms associated with the token and priority, along with the error detection and recovery mechanisms that are the key attributes of a ring structure. [Ref. 13: p. 12-13]

Physical layerprotocols associated with token rings can result in a duplex station interface: a station on the ring can transmit and receive information at the same time. This implies that every active station is continuously monitoring the information being received from the upstream station. [Ref. 13: p. 12-13]

Point-to-point transmission also is enabled. Information propagates sequentially from station to station. The ring protocols allow for each station to identify the active station that is immediately upstream. Closed communication paths are possible. Every station is physically downstream from all other stations, thereby permitting a single transmission from any station to be received by multiple stations. [Ref. 13: p. 12-13]

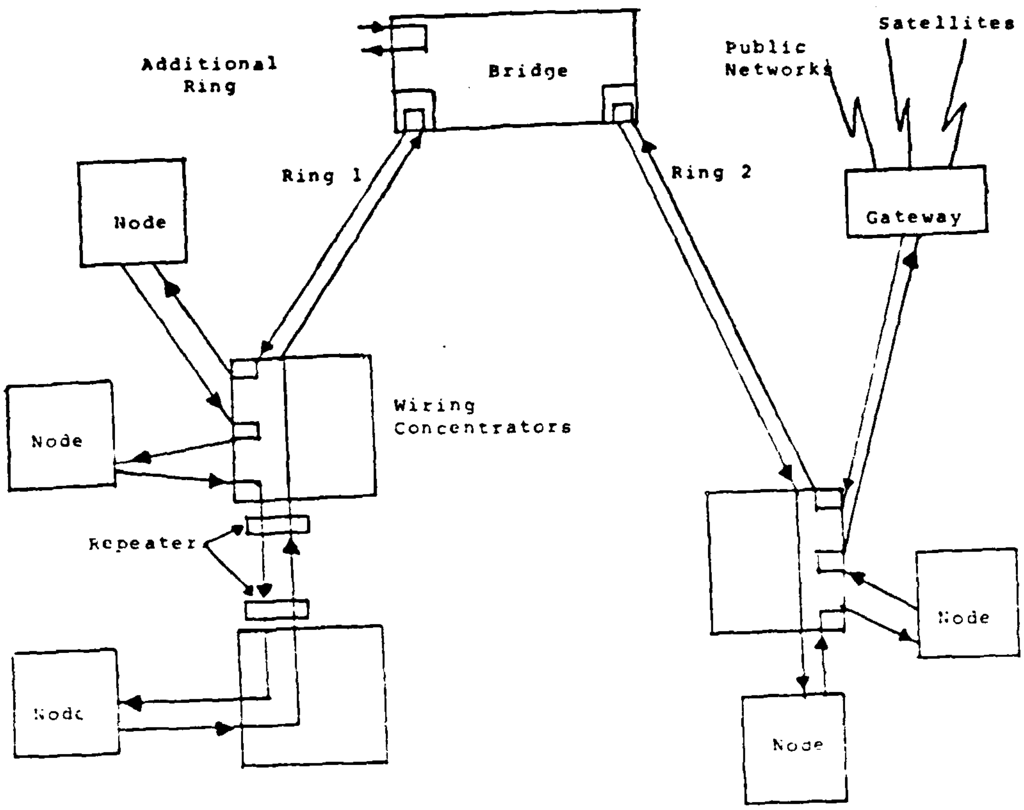
Ring networks typically employ baseband transmission technology using shielded twisted-pair cable. This offers many advantages, including electromagnetic noise immunity due to the blanced nature of the transmission medium, and the use of primarily digital logic to control access to the medium as opposed to analog logic. [Ref. 13: p. 12-13] Figure 11 on page 38 illustrates a typical token-ring architecture.

Token passing schemes have been used in star, bus, and ring networks. In token passing bus networks, the time for a token to pass from one node to another includes the propagation time on the bus and the time for the receiving node to recognize the token. If this interface time is long, the time for a token to travel around the logical network will be significant. Thus each packet may have a significant overhead delay, even in light traffic conditions. [Ref. 16: p. III-34]

Token passing ring networks use repeaters on each node. As a result, incoming information is passed on to the next node without any processing delay. With less than 2000 nodes, the propagation delay is not significant, and the ring network is normally superior to the token passing bus network. The sending nodes have the extra responsibility of removing their data after the packet has traversed the entire ring and returned to the original sending node. More complex circuitry is needed to handle this function. [Ref. 16: p. III-34]

6. Comparsion of CSMA/CD and Token Passing

Based on the analytical results, token passing via a ring is the least sensitive to workload, offers short delays under light loads, and offers slightly longer delays under heavy load. Token passing via a bus has the longest delay under light loads, cannot



*Wiring concentrators permit flexible wiring of building
*and bypass of faults.

*Bridges interconnect rings in campus and other environments
with many terminals.

*Gateways interconnect to the Wide Area Network environment.

Figure 11. Token-Ring Architecture

carry as much traffic as a ring under heavy loads, and is quite sensitive to propagation time. CSMA/CD offers the shortest delay under light loads, and is sensitive to traffic loads and propagation time in the bus. [Ref. 16: p. III-35] Table 2 provides a comparison of CSMA/CD and token ring topologies.

Table 2. COMPARISION OF CSMA/CD AND TOKEN PASSING TOPOLOGIES

Category	CSMA/CD	Token Passing
Expandability	Good	Need network reconfiguration
Survivability	Good	Good if monitor function can be resumed in a decentralized way when the active monitor fails
Priority	Can only be implemented in backoff time	Easy to implement
Medium Utilization	Good in light traffic, poor in heavy traffic	Good in heavy traffic, poor in light traffic
Packet delay	Short in light traffic, very long in heavy traffic	Not too sensitive to traffic load, but a little longer delay in heavy traffic

7. Performance Issues

In general, the user of a LAN is concerned only with three things. First, the necessary hardware must be available to allow the system to be physically connected to the network. Second, the system must have the appropriate software required for accessing the services supported by the network (electronic mail, file archiving, etc.). Third, access time to these services must be within acceptable limits. The overall end-to-end performance of any computer communication network is likely to be dominated by the delays experienced in the higher protocol layers rather than any small variations that may be caused by the different LAN topologies and MAC methods. Nevertheless, since the different types of LAN clearly have varying operational characterstics, these differences are important for the network designer. [Ref. 4: p. 243]

In general, good design practice will ensure that the capacity of any LAN is more than adequate to handle the aggregate mean offered load of its users. Conversely, it is bad practice to try to operate a network near its total capacity since, under these conditions, predictably long delays at the network interface are inevitable and end-to-end response time will rapidly rise above the maximum level which is acceptable to the system's users. This is especially the case with a CSMA/CD protocol. Its performance under heavy offered loads is relatively unstable: as the offered load increases to the point at which the network utilization starts to become a significant proportion of its maximum capacity, so the probability of collisions will also increase. Of course with heavy offered loads this is also the case with a token-based protocol since, as the transmission medium approaches saturation, only high priority frames will be transmitted and lower priority frames will be queued indefinitely. [Ref. 4: p. 243]

It should be stressed that, even with a small mean offered load and a cable bandwidth of, say, 10Mbps, the maximum end-to-end data transfer rate associated with a particular user transaction is likely to be nearer to tens of kilobits because of the processing delays associated with the higher protocol layers. Providing the aggregate mean offered load remains only a modest fraction of the cable bandwith, however, many user transactions at this rate can be in progress concurrently. [Ref. 4: p. 243]

IV. OPTIMAL LAN FOR ROCN

A. INTRODUCTION

Growth in computer communications in the ROC is desirable if it is steady and purposeful. If growth is too slow or is disorderly, then the ROC will not keep pace with the rest of the world. Growth of computer communications for the military also is critical. Growth that is either too slow or of poor quality will harm national military progress.

LAN systems must be considered for future ROCN computer communication systems. Requirements for installation, support, and maintenance of network equipment should be seriously considered. The current communication system of the ROCN has been described in Chapter I. The basic concept of data communication has been analyzed in Chapter II, and the design of LANs is covered in Chapter III. The future growth requirements for the ROCN LAN are emphasized in this chapter.

B. OBJECTIVE OF THE ROCN LAN SYSTEM

The major mission of the ROCN is to maintain the peace of the Western Pacific region and to defend against Communist China aggression. To do this the ROCN must have modern advanced weapons, and must maintain a state of combat readiness at all times. During war time, shipboard LANs can provide accurate, rapid, reliable, and secure intelligence, ensuring combat efficiency. During peace time, shipboard LANs can provide efficient document management and knowledge sharing, enhancing information transfer. However, first ROCN LAN systems must reach a level of working efficiency and the ability to meet the needs of combat readiness at any time.

Every male ROC citizen has an obligation to be a soldier. While ashore, computers can integrate military knowledge with revelant specific civilian knowledge. Small dedicated minicomputers or microcomputers, the trend of the future, will assist in this process.

C. REQUIREMENTS

In Taiwan, both manpower and monetary resources require the use of computers for the planning and implementation of programs related to possible future altercations. Computers also will raise executive efficiency and improve the working environment.

important in the modern world. The following requirements must be met for any ROCN LAN system.

- Budget
- Training and maintenance
- Security
- Reliability
- Efficiency
- Survivability
- Performance.

1. Budget

Funds must be allocated based on performance and on need; money cannot be spent that is not available. Many budget issues arise when installing LAN equipment. These include:

- What is the system minimum cost?
- Who will support this system?
- Who will pay for training?
- Who will pay for maintenance and spare parts?

Funds must be carefully allocated, controlled, and utilized by an able staff which has computer assets if possible. Poor distribution and use of funds have caused many failures. In addition, once purchased, the equipment is plant property and must be accounted for accordingly.

2. Training and Maintenance

The ROC Naval Academy is responsible for training students in data communication concepts. The ROCN Electronic Communication School and Weapon School are responsible for training users in the operation of LANs. Many sources of help are available. These include:

- Individuals who set up the training program.
- Vendors of computer equipment used in training.
- Commercial training consultants.
- Experienced personnel from the command or from neighboring commands.

Maintenance is not usually a major problem with small computing systems. If these systems are operated properly in a relatively clean, cool environment, few problems

should be encountered. However, protection against brown-outs and power fluctuations is important. Also, the user must protect Navy warranty rights, and careful inspection of service and operating requirements is necessary to protect those rights. Maintenance requires the following.

- Mainentanence training for unit personnel.
- One-time purchase request (on-site as well as carry-in) that includes appropriate warranties.
- Preventive maintenance as part of each day's routine work, such as head cleaning and enclosure dusting.

Purchase of additional standby equipment should be considered. Because outage of the LAN at a Naval base or at sea is a possibility, spare hardware is necessary.

3. Security

ROC Naval base and shipboard LANs will be used to help manage such things as documents, record rosters, security rosters, training records, and many other types of personnel information. The LAN multiplies the problems of affording appropriate levels of protection for personal and intelligence information. Data on a network medium is not automatically safe from enemies and intruders. Several safeguards must be used to ensure security. Special database software which affords passwording and file security may have to be acquired. Restricting access to a LAN to particular persons may be necessary. Appropriate physical security of backup tapes, diskette media, and the like must be provided.

LANs used in military environments should provide different security levels, based on subscriber needs. For multilevel subscribers, communication should be restricted according to the ROC DoD security policy constraints. Basically, ROC DoD security levels are divided as shown below:

- Unclassified
- Confidential
- Restricted
- Secret
- Top secret.

Security of classified data is critical for the military. Complex ciphertext may be needed. In general, a shipboard LAN will not be authorized for the processing of classified information and steps to prevent such processing must be taken. If the system

provides communication external to the ship, special steps must be taken to insure that unauthorized access to the system is prevented.

4. Reliability

One of the characterics of a LAN must be low error rate, since reliability is one of the most important requirements for data communication. The transmission medium and access methods associated with different topologies will produce different levels of reliability. Thus the error detection technique must be tested and considered before installing a LAN system. If the receiver of data cannot read or believe it, the system is useless.

5. Efficiency

Econonies of scale play an important role in any computer system. Economic efficiency means allocating resources in the best manner among the various types of work stations, printers, and computer peripherals that make up the system. The simplest possible techniques are the best.

Computer and data communication functions can be applied to various aspects of social and economic life. The best systems are modular, ensuring that they will not require replacement all at once and can be kept modern as some peripherals change. Due to the rapid pace of technological change in the computer and communication industries, data processsing and information sharing techniques change rapidly. The throughput of a LAN is directly related to the access method, processing capacity, and transmission medium at each network node. A high speed data rate is desirable, and the system must be compatible for interconnection with long distance networks, if possible.

6. Survivability

All equipment used by the military must be survivable. LANs used for the ROCN should take into account the following.

- LANs should be designed for unattended operation, and be located at or near the subscriber sites they support. [Ref. 17: p. 154]
- They should be protected from high amplitude electromagnetic pulses, and uninterruptable power supplies should be provided. [Ref. 17: p. 154]
- In the war time, should some parts of the equipment fail or be damaged, the rest of the LAN equipment should work as usual.
- Should the enemy sabotage the LAN's transmission medium, rapid repair or replacement should be possible.

7. Performance

Many studies have determined that the single most important factor in determining network performance is the type of access method employed [Ref. 18: p. 154]. For optimum LAN performance on shipboard, it is necessary to investigate and make comparisons between the most commonly used multiple access control protocols which can be used to control network access. Each of the three possible topologies should be examined to determine which provides the best performance, as part of the process of deciding which LAN is most appropriate for shipboard use.

Bus and ring topologies are good for LANs, as discussed in Chapter II. Some topologies that utilize the CSMA/CD method perform better under applications where short-burst traffic is characteristic, while token passing access methods provide relatively better performance when the network has a heavy load. [Ref. 18: p. 154]

Figure 12 on page 46, Figure 13 on page 47, Figure 14 on page 48, Figure 15 on page 49, Figure 16 on page 50, and Figure 17 on page 51 provide the maximum data rates and throughput rates needed to make comparsions. Several assumptions are made, for these comparisons:

- There are two delay regimes, low delay and high delay.
- Ring topology uses only token passing access for control and all nodes are equidistant apart.
- Bus topologies can use token passing or CSMA access methods.
- There are 100 nodes. At low delay one node is on line and sending traffic. At high delay 100 nodes are on line and sending traffic.
- All frames consist of a header and a trailer with a total of 96 control bits.
- The total bit count for a frame is 500, 1000, or 2000 bits including control and data bits.

The following conclusions can be drawn by examining the plots:

- Token ring is the least sensitive to workload.
- Token ring offers short delay under light load.
- Token ring offers controlled delay under heavier loads.
- Token bus has the greatest delay under light load.
- Token bus cannot handle as much traffic as a ring under heavy load.
- CSMA offers very low delay under light load.
- CSMA is quite sensitive to the heavy work load.

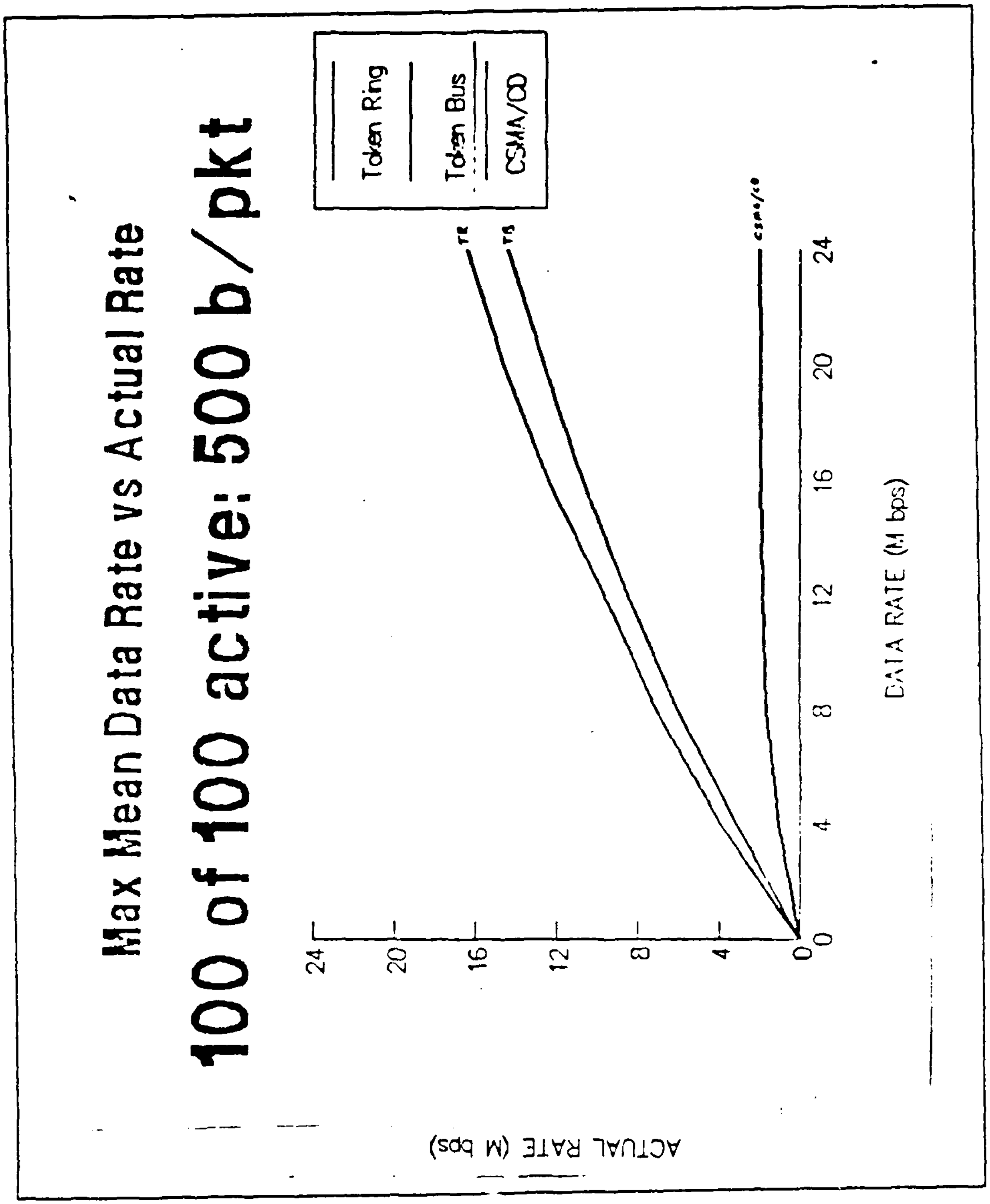


Figure 12. Comparison of Token Ring, Token Bus, and CSMA/CD Topologies When all Nodes are Actives, at 500 Bits per Packet

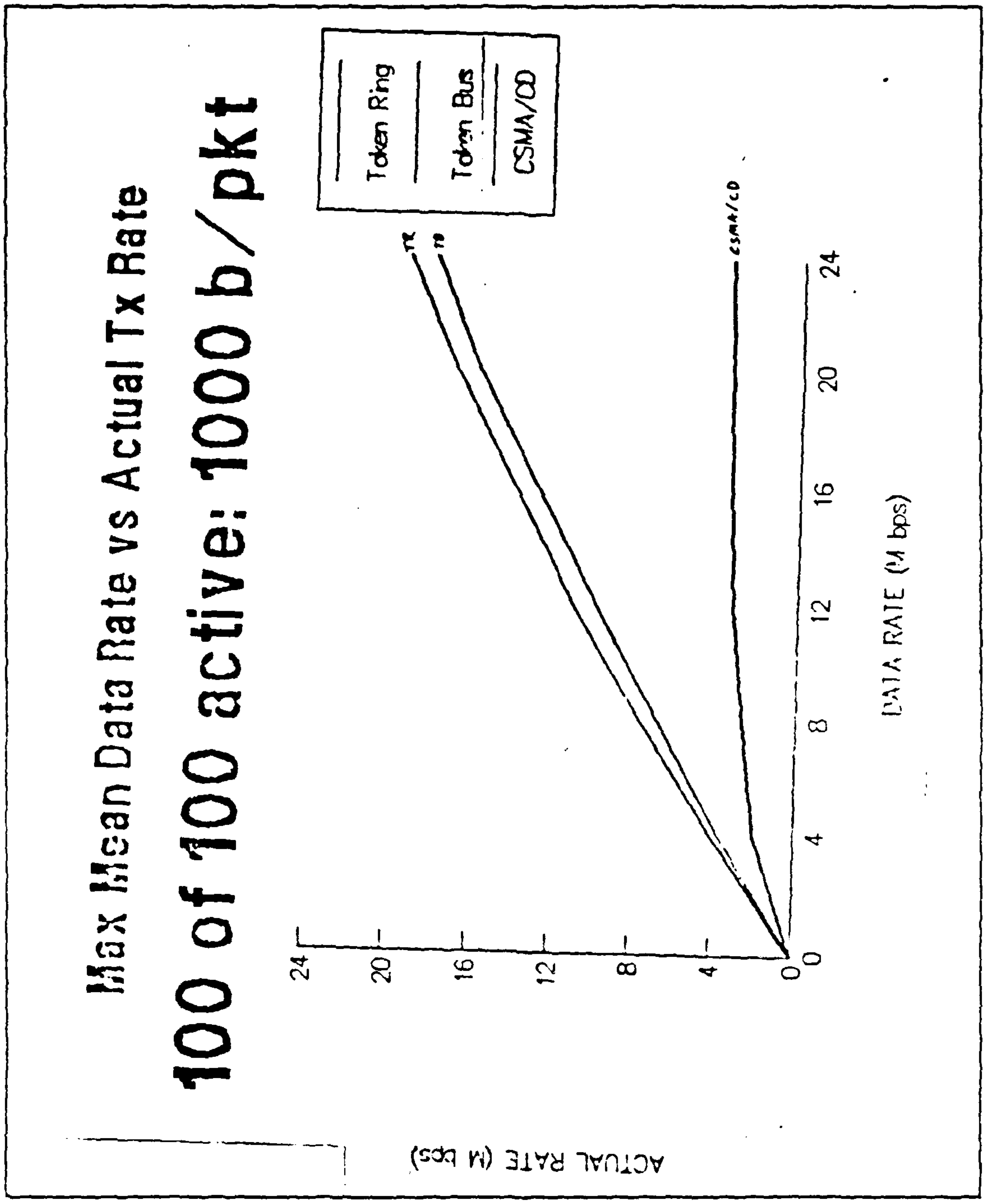


Figure 13. Comparison of Token Ring, Token Bus, and CSMA/CD Topologies When all Nodes are Actives, at 1000 Bits per Packet

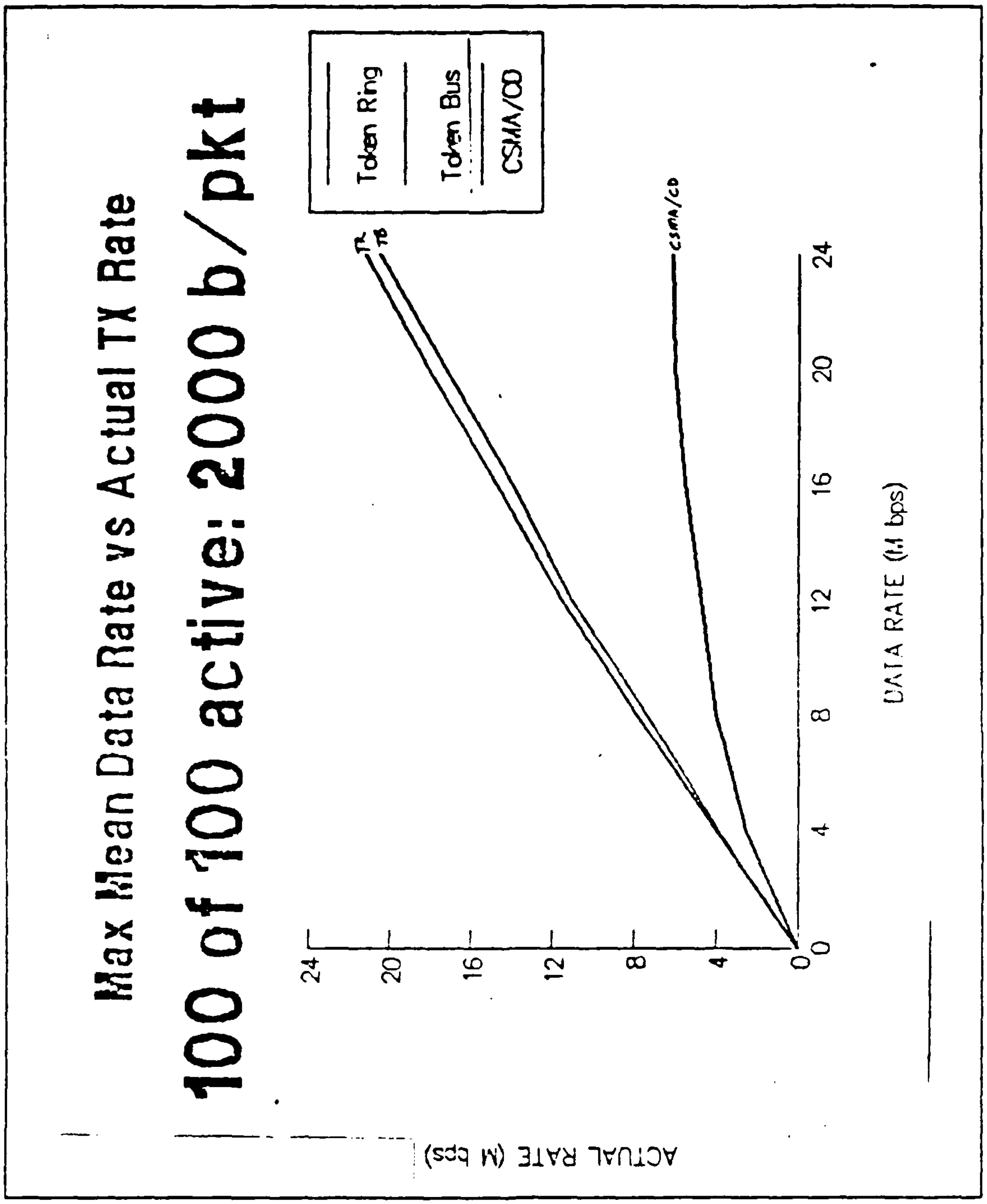


Figure 14. Comparison of Token Ring, Token Bus, and CSMA/CD Topologies When all Nodes are Actives, at 2000 Bits per Packet

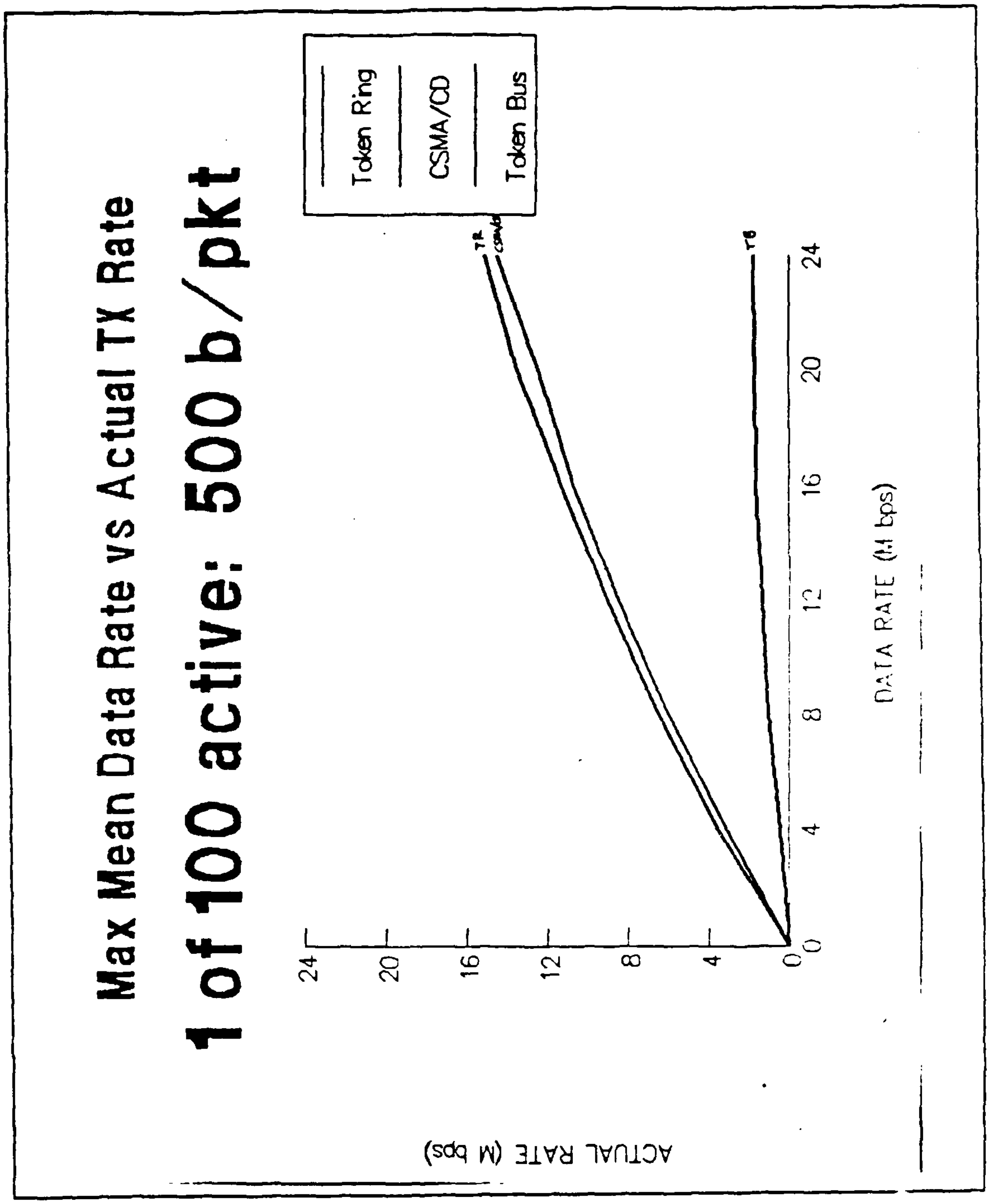


Figure 15. Comparison of Token Ring, Token Bus, and CSMA/CD Topologies When Only One Node Out of 100 is Active, at 500 Bits per Packet

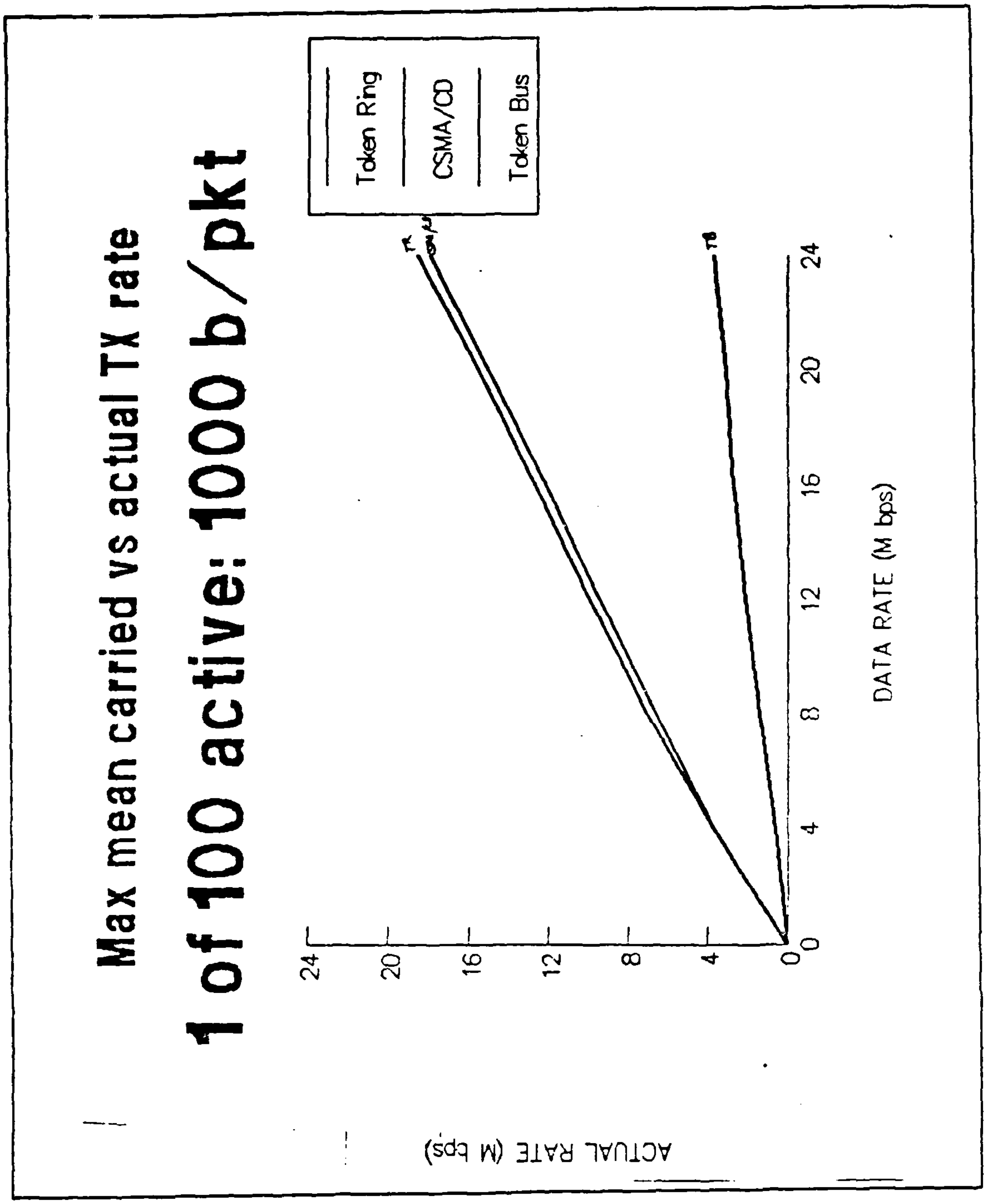


Figure 16. **Comparison of Token Ring, Token Bus, and CSMA/CD Topologies, One Node Out of 100 Active, at 1000 Bits per Packet**

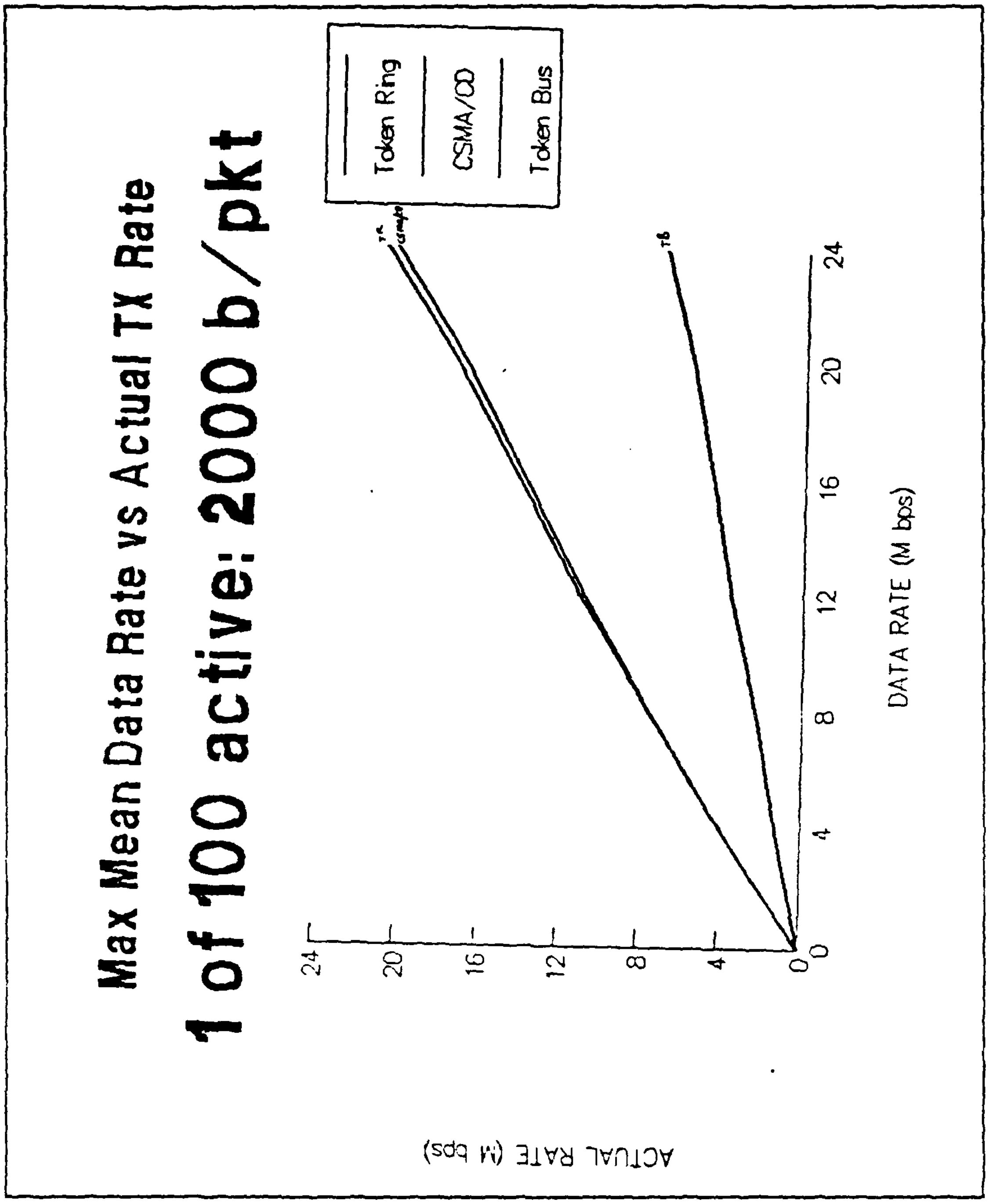


Figure 17. Comparison of Token Ring, Token Bus, and CSMA/CD Topologies, One Node Out of 100 Active, at 2000 Bits per Packet

Based on this information, one can conclude that optimum performance must be considered before installing LANs in the ROCN.

V. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

This study has clearly defined the ROCN goal and described the ROCN current communication problems in Chapter I. The basic concept of data communication has been discussed in Chapter II. Two popular LAN models and some practical computer standards and architectures have been provided in Chapter III. LAN requirements for the ROCN have been discussed in Chapter IV.

As noted, the advent of integrated circuits has drastically reduced the size, cost, and electrical drain of desk-size microcomputers. Integrating computers and developing computer communication have become critically important for modern nations. The ROC is among the ranks of newly developed countries in the world, and it has the ability to produce its own microcomputers and computer networks.

Token ring and Ethernet (CSMA/CD) are two network architectures that would be appropriate for ROC and ROCN high-speed, low-error rate LANs, as discussed in Chapter III. Which is best depends on the situation, as described there.

Computers will be useful for integrating civilian and military knowledge in Taiwan, as discussed in Chapter IV. The requirements for an effective LAN for the ROCN also have been provided there. Introducing new computer communication technologies and computer equipment to the ROCN is a very important course for the future, as long as the resulting systems meet critical ROCN goals.

B. RECOMMENDATIONS

If you don't know where you are going, it is very difficult to get there and extremely difficult to determine that where you are is where you want to be. Throughout human history the success of planning large and small projects can be traced to the clarity with which goals were defined.

Goals must be realistic and attainable. They must be desirable in terms of reasonableness and necessity, and stated in specific, observable, measurable terms. Determining the ROCN's primary goals is important before installing ground-based and shipboard LANs. Goals such as adequate traning for LAN use and proper maintenance of these systems can be achieved if the ROCN considers all necessary information on present status and future needs.

The ROC should cooperate with the U.S. for technology development to help ensure comparability, competition, and growth, which are necessary for the future of the ROCN. At the same time, support from the U.S. government is important if the ROC is to meet its goals.

Computer systems and networks should be developed to be as simple and uncomplicated as possible. Since the use of different brands of computers introduces complexities and compatibility problems for interconnecting WANs and LANs, this should be avoided if possible. Meeting to discuss software and protocols will result in new ideas and encourage growth of the civilian computer industry.

Military switching offices and civilian switching offices are separated in Taiwan; telephone lines are also separate. For now, LANs interconnecting with LANs on Naval bases should use existing military telephone lines. LANs interconnected with WANs should consider using civilian telephone lines.

Different network access methods associated with different topologies result in different levels of performance in LAN systems. Therefore, before installing LANs, the ROCN must decide what kind of performance is required for the future. Security factors also must be seriously considered. Budgets, reliability, and efficiency must be considered. Once installed, ROCN must plan to test and evaluate the resulting security and survivability of the systems. Reports of the results can be discussed and used to improve the ROCN LAN systems in the future.

APPENDIX GLOSSARY

CCITT	Consultative Committee on International Telegraphy and Telephone
CPU	Central processing unit
CSMA	Carrier sense multiple access
CSMA/CD	Carrier sense multiple access with collision detection
DAP	Data access protocol
DEC	Digital Equipment Corporation
DNA	Digital network architecture
DoD	Department of Defense
DPA	DoD protocol architecture
ECMA	European Computer Manufacturers Association
FDMA	Frequency division multiple access
FMD	Function management data services
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet protocol
ISO	International Standards Organization
LAN	Local area network
LCC	Logical link control
MAC	Medium access control
NAU	Network addressable unit
NSP	Network services protocol
OSI	Open Systems Interconnection
PBX	Private Branch Exchange
ROC	Republic of China
ROCN	Republic of China Navy
SNA	System network architecture
TCP	Transmission control protocol
TDMA	Time division multiple access
TP	Transport protocol
WAN	Wide area network

LIST OF REFERENCES

1. Loomis, M.E.S., *Data Communications*, Prentice-Hall Inc., 1983.

2. McGlynn, D.R., *Distributed Processing and Data Communication*, John Wiley and Sons, Inc., 1978.

3. Schneidewind, N.F., " Interconnecting Local Networks to Long Distance Networks, " *Computer*, Vol. 16, No. 9, September 1983.

4. Halsall, F., *Introduction to Data Communications*, Addison-Wesley Publishing Company, 1985.

5. Tanenbaum, A.S., *Computer Networks*, Prentice-Hall Inc., 1981.

6. Stallings, W., *Data and Computer Communications*, Macmillan Publishing Company, New York, 1985.

7. Well, J.D., *IBM's Token-ring LAN (Local Area Network), A Base-level Communications Solution*, student report, Air Command and Staff College, Maxwell Air Force Base, Alabama April 1984.

8. Golesh, D., *Introduction to Local Area Networks*, Digital Equipment Corportation, Marynard Mass., 1984.

9. Taub, H., and Schilling, D.L., *Principles of Communications Systems*, McGraw-Hill Book Company, 1986.

10. Goos, G., and others, *Local Area Networks: An Advanced Course*, Springer-Verlag, Berlin, 1985.

11. Luczak, E.C., *Global Bus Computer Communications Techniques*, Computer Networking Symposium, IEEE, Gaithersburg Maryland, December 1978.

12. Ulm, M. J., *7th Conference on Local Computer Networks,* IEEE Computer Society, Sliver Spring MD., October 11-13, 1982.

13. Strole, N. C., " The IBM Token Ring Network, a Functional Overview, " Vol. 1, No. 1, *IEEE Network Magazine,* January 1987.

14. *The Defense Data Network Course,* Network Strategies Inc., Fairfax VA., April, 1986.

15. Lam, S. S., *Principles of Communication and Networking Protocols,* IEEE, 1984.

16. Yeh, J., and others, *Local Area Networks: An Advanced Course: Technology, Products, and Trends,* U.S. Navy Laboratories Carderock, Maryland, January 11, 1985.

17. Fidelman, M.R., and others, " Survivability of the Defense Data Network, " *Signal,* May 1986.

18. Lundquist, C.Q., " Handbook for Local Area Networks, " *Computer,* June 1985.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center Cameron Station Alexandria, VA 22304-6145	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, CA 93943-5002	2
3.	Department Chairman, Code 54 Department of Administrative Sciences Naval Postgraduate School Monterey, CA 93943-5000	1
4.	Professor Judith H. Lind, Code 55 Li Department of Operation Research Naval Postgraduate School Monterey, CA 93943-5000	2
5.	Professor Dan C. Boger, Code 54 Bo Department of Administrative Sciences Naval Postgraduate School Monterey, CA 93943-5000	1
6.	Naval Academy Library Kaoshiung Tsoying P.O.Box 8494 Taipei Republic of China on Taiwan	3
7.	Feng, Yen Chun SMC 1506 Naval Postgraduate School Monterey, CA 93943	1
8.	Wang, Ming Hua SMC 2267 Naval Postgraduate School Monterey, CA 93943	2
9.	Hsu, Ta Chieh SMC 1372 Naval Postgraduate School Monterey, CA 93943	1

10. Kao, Chang Lung 2
SMC 2408
Naval Postgraduate School
Monterey, CA 93943

11. Chia, Hua Kai 1
SMC 1919
Naval Postgraduate School
Monterey, CA 93943

12. Feng, Cheng Chuan 2
SMC 1353
Naval Postgraduate School
Monterey, CA 93943

13. Wang, Nai 5
Kaoshiung Tsoying
12, Lane 18 Ta Road
Taipei, Taiwan (ROC)